



# **Symantec Endpoint Protection Installation and Administration Guide**

**December 2020**

---

# Table of Contents

<b>Release Notes.....</b>	<b>27</b>
What's new for Symantec Endpoint Protection 14.3 RU2?.....	27
System requirements for Symantec Endpoint Protection (SEP) 14.3 RU3.....	30
Known issues and workarounds for Symantec Endpoint Protection (SEP).....	38
Supported virtual installations and virtualization products.....	45
About Endpoint Protection release types and versions.....	46
Where to get more information.....	47
What's new for all releases of Symantec Endpoint Protection (SEP) 14.x.....	48
What's new for Symantec Endpoint Protection 14.3 RU1 MP1.....	58
What's new for Symantec Endpoint Protection 14.3 RU1?.....	58
What's new for Symantec Endpoint Protection 14.3 MP1 (14.3.0.1).....	63
What's new for Symantec Endpoint Protection 14.3?.....	64
<b>What is Symantec Endpoint Protection?.....</b>	<b>66</b>
How Symantec Endpoint Protection technologies protect your computers.....	66
Symantec Endpoint Protection architecture components.....	69
<b>Getting Started.....</b>	<b>71</b>
Symantec Endpoint Protection Quick Start Guide.....	75
Installing Symantec Endpoint Protection Manager.....	79
Configuring Symantec Endpoint Protection Manager after installation.....	80
Installing Symantec Endpoint Protection Manager with a custom configuration.....	81
Logging on to the Symantec Endpoint Protection Manager console.....	83
Activating or importing your Symantec Endpoint Protection product license.....	86
Purchasing Symantec Endpoint Protection licenses.....	89
Installing Symantec Endpoint Protection clients with Save Package.....	90
Installing the Symantec Endpoint Protection client for Mac.....	91
About authorizing system extensions for Symantec Endpoint Protection for macOS 10.15 or later.....	92
Managing kernel extension authorization when deploying the Symantec Endpoint Protection client for Mac.....	92
Installing the Symantec Agent for Linux or the Symantec Endpoint Protection client for Linux.....	93
Getting started on the Linux agent.....	95
About auto-compile for the Symantec Endpoint Protection client for Linux.....	96
About the Linux client graphical user interface.....	97
Installing Symantec Endpoint Protection clients with Remote Push.....	98
Installing Symantec Endpoint Protection clients with Web Link and Email.....	100
What do I do after I install the management server?.....	101
Communication ports for Symantec Endpoint Protection.....	103

---

<b>Installing and Uninstalling the Management Server and Clients.....</b>	<b>106</b>
Network architecture considerations.....	106
About choosing a database type.....	107
About basic management server settings.....	107
About SQL Server configuration settings.....	108
About SQL Server database authentication modes.....	111
Internationalization requirements.....	112
Uninstalling Symantec Endpoint Protection Manager.....	113
<b>Managing the Symantec Endpoint Protection client installation.....</b>	<b>113</b>
Preparing Windows and Mac computers for remote deployment.....	114
Choosing a method to install the client using the Client Deployment Wizard.....	116
Choosing which security features to install on the client.....	117
Managing client installation packages.....	117
Exporting client installation packages.....	118
Importing client installation packages into Symantec Endpoint Protection Manager.....	119
Windows client installation package and content update sizes.....	120
Creating custom Windows client installation packages in Symantec Endpoint Protection Manager.....	121
About the Windows client installation settings.....	121
Customizing the client installation settings.....	122
Uninstalling existing security software.....	122
Choosing whether to download cloud-based or local-based definitions using the client installation type.....	124
Third-party security software removal in Endpoint Protection 14.....	125
Third-party security software removal in Symantec Endpoint Protection 14.3 RU1 and later.....	125
Restarting the client computers from Symantec Endpoint Protection Manager.....	127
About managed and unmanaged clients.....	128
How to get an unmanaged client installation package.....	129
Installing an unmanaged Windows client.....	130
About uninstalling the Symantec Endpoint Protection client.....	131
Uninstalling the Symantec Endpoint Protection client for Windows.....	132
Uninstalling the Symantec Endpoint Protection client for Mac.....	132
Uninstalling the Symantec Agent for Linux or the Symantec Endpoint Protection client for Linux.....	133
<b>Upgrading and Migrating to the Latest Release of Symantec Endpoint Protection (SEP).....</b>	<b>135</b>
Upgrade best practices for Endpoint Protection 14.x.....	136
Supported and unsupported upgrade paths to the latest version of Symantec Endpoint Protection 14.x.....	140
Increasing Symantec Endpoint Protection Manager available disk space before an upgrade.....	141
Upgrading a management server.....	142
Best practices for upgrading from the embedded database to the Microsoft SQL Server Express database...	143
Reducing the database size when the database is full before an upgrade to Microsoft SQL Server Express...	145
Enabling FILESTREAM for the Microsoft SQL Server database.....	146

---

---

Reducing the database size to less than 10 GB before an upgrade to Microsoft SQL Server Express.....	147
Making more disk space available to upgrade to the default Microsoft SQL Server Express database.....	149
Configuring encrypted communication between Symantec Endpoint Protection Manager and Microsoft SQL Server.....	150
Upgrading an environment that uses multiple embedded databases and management servers.....	158
Stopping and starting the management server service.....	158
Preventing replication during an upgrade.....	159
Restoring replication.....	160
Choosing which method to upgrade the client software.....	160
Upgrading client software with AutoUpgrade.....	162
Applying AutoUpgrade settings to other groups.....	164
Upgrading Symantec Endpoint Protection 14.3 RU2+ to a supported language.....	164
Installing Endpoint Protection client patches on Windows clients.....	165
Upgrading the Symantec Linux Agent.....	166
Updating the kernel modules for the Symantec Linux Agent.....	167
Upgrading Group Update Providers.....	168
Upgrade resources for Symantec Endpoint Protection.....	169
<b>Licensing Symantec Endpoint Protection.....</b>	<b>170</b>
Checking the license status in Symantec Endpoint Protection Manager.....	171
Backing up and recovering your license file (.slf).....	171
Purging obsolete clients from the database to make more licenses available.....	172
What does a Symantec Endpoint Protection license cover?.....	172
About multi-year licenses.....	173
Symantec Endpoint Protection product license terminology.....	173
Licensing an unmanaged Windows client.....	174
<b>Managing the client-server connection.....</b>	<b>175</b>
<b>Configuring management servers and the server-client connection.....</b>	<b>175</b>
Setting up HTTPS communications between a Symantec Endpoint Protection Manager and the clients.....	175
Verifying port availability.....	176
Changing the HTTPS port for Apache for client communication.....	176
Enabling HTTPS client-server communications.....	177
Improving client and server performance.....	179
About server certificates.....	180
Best practices for updating server certificates and maintaining the client-server connection.....	181
Update the server certificate on the management server without breaking communications with the client... ..	182
Updating or restoring a server certificate.....	184
Reconfiguring Symantec Endpoint Protection Manager after changing the computer's IP address and host name.....	185
Checking whether the client is connected to the management server and is protected.....	186
Symantec Endpoint Protection client status icons.....	188

---

---

Using the policy serial number to check client-server communication.....	188
Updating policies and content on the client using push mode or pull mode.....	189
How does the client computer and the management server communicate?.....	190
How do I replace the client-server communications file on the client computer?.....	192
Restoring client-server communications with Communication Update Package Deployment.....	193
Exporting the client-server communications file (Sylink.xml) manually.....	194
Importing client-server communication settings into the Windows client.....	195
Importing client-server communication settings into the Linux client.....	195
IPv6 networking support.....	196
<b>Managing Groups, Clients, Administrators, and Domains.....</b>	<b>197</b>
<b>Managing groups of clients.....</b>	<b>197</b>
How you can structure groups.....	198
Adding a group.....	198
Importing existing groups and computers from an Active Directory or an LDAP server.....	199
About importing organizational units from the directory server.....	199
Connecting Symantec Endpoint Protection Manager to a directory server.....	200
Connecting to a directory server on a replicated site.....	201
Importing organizational units from a directory server.....	202
Disabling a group's inheritance.....	202
Blocking client computers from being added to groups.....	203
Moving a client computer to another group.....	203
<b>Managing client computers.....</b>	<b>204</b>
Viewing the protection status of client computers.....	205
Enabling protection on the client computer.....	206
Searching for the clients that do not have the client software installed.....	206
Searching for information about client computers.....	207
What are the commands that you can run on client computers?.....	207
Running commands on client computers from the console.....	209
Ensuring that a client does not restart.....	210
Switching a Windows client between user mode and computer mode.....	210
Configuring a client to detect unmanaged devices.....	211
Password-protecting the Symantec Endpoint Protection client.....	212
Preventing and allowing users to change the client's user interface.....	213
Collecting user information.....	214
Checking on your Mac client using AppleScript scripts.....	215
Managing your Linux client using the command line tool (sav).....	216
<b>Managing remote clients.....</b>	<b>217</b>
Managing locations for remote clients.....	218
Enabling location awareness for a client.....	220
Adding a location to a group.....	221

---

---

Changing a default location.....	221
Setting up Scenario One location awareness conditions.....	222
Setting up Scenario Two location awareness conditions.....	224
Configuring communication settings for a location.....	225
About strengthening your security policies for remote clients.....	226
Best practices for Firewall policy settings for remote clients.....	226
About turning on notifications for remote clients.....	227
About monitoring remote clients from the management server.....	227
Monitoring roaming Symantec Endpoint Protection clients from the cloud console.....	228
<b>Managing administrator accounts.....</b>	<b>229</b>
About administrator accounts and access rights.....	230
Adding an administrator account and setting access rights.....	232
Choosing the authentication method for administrator accounts.....	232
Using RSA SecurID authentication with Symantec Endpoint Protection Manager.....	233
Configuring two-factor authentication with Symantec VIP.....	235
Configuring Symantec Endpoint Protection Manager to authenticate administrators who log on with smart cards.....	235
Testing directory server authentication for an administrator account.....	237
Changing the password for an administrator account or the default database.....	240
Resetting a forgotten Symantec Endpoint Protection Manager password.....	241
Displaying the <b>Forgot your password?</b> link so that administrators can reset lost passwords.....	242
Enabling Symantec Endpoint Protection Manager logon passwords to never expire.....	242
Displaying a message for administrators to see before logging on to the Symantec Endpoint Protection Manager console.....	243
Displaying the <b>Remember my user name</b> and <b>Remember my password</b> check boxes on the logon screen.....	243
Granting or blocking access to remote Symantec Endpoint Protection Manager consoles.....	244
Unlocking an administrator's account after too many logon attempts.....	245
Changing the timeout period for staying logged on to the Symantec Endpoint Protection Manager console.....	245
<b>About domains.....</b>	<b>246</b>
Adding a domain.....	247
Switching to the current domain.....	248
<b>Using Policies to Manage Security.....</b>	<b>249</b>
<b>Performing the tasks that are common to all policies.....</b>	<b>249</b>
The types of security policies.....	250
Updating client policies.....	252
Adding a policy.....	252
Editing a policy.....	253
Finding a policy's default settings.....	253
Copying and pasting a policy on the <b>Policies</b> page.....	254
Copying and pasting a policy on the <b>Clients</b> page.....	254

---

---

Assigning a policy to a group or location.....	255
Replacing a policy.....	256
Exporting and importing individual Endpoint Protection policies.....	256
About shared and non-shared policies.....	257
Converting a shared policy to a non-shared policy.....	258
Unassigning a policy from a group or location.....	258
Preventing users from disabling protection on client computers.....	259
Monitoring the applications and services that run on client computers.....	262
Enabling application learning.....	263
Searching for information about the learned applications that the computers run.....	264
<b>Managing firewall protection.....</b>	<b>265</b>
How a firewall works.....	266
About the Symantec Endpoint Protection firewall.....	266
About firewall settings for the Mac client.....	267
Creating a firewall policy.....	268
Managing firewall rules.....	270
Adding a new firewall rule.....	271
About firewall server rules and client rules.....	272
About the firewall rule, firewall setting, and intrusion prevention processing order.....	273
About inherited firewall rules.....	274
Changing the order of firewall rules.....	275
How the firewall uses stateful inspection.....	276
About firewall rule application triggers.....	276
About firewall rule host triggers.....	279
Adding host groups.....	280
About firewall rule network services triggers.....	281
Adding network services to the default network services list.....	281
About firewall rule network adapter triggers.....	282
Adding a custom network adapter to the network adapter list.....	282
Importing and exporting firewall rules.....	283
Importing or exporting firewall rules on the client.....	284
Customizing firewall rules.....	284
Configuring firewall settings for mixed control.....	291
Enabling communications for network services instead of adding a rule.....	292
Automatically blocking connections to an attacking computer.....	293
Detecting potential attacks and spoofing attempts.....	293
Preventing outside stealth attacks on computers.....	294
Disabling the Windows Firewall.....	295
<b>Managing intrusion prevention.....</b>	<b>296</b>
How intrusion prevention works.....	298

---

---

About Symantec IPS signatures.....	298
About custom IPS signatures.....	299
Creating exceptions for IPS signatures.....	299
Setting up a list of excluded computers.....	301
Enabling network intrusion prevention or browser intrusion prevention.....	301
Integrating browser extensions with Symantec Endpoint Protection to protect against malicious websites.....	302
Configuring client notifications for intrusion prevention and Memory Exploit Mitigation.....	308
Managing custom intrusion prevention signatures.....	308
Creating a custom IPS library.....	309
Adding signatures to a custom IPS library.....	310
Changing the order of custom IPS signatures.....	311
Defining variables for custom IPS signatures.....	312
Assigning multiple custom IPS libraries to a group.....	312
Testing custom IPS signatures.....	313
<b>Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy.....</b>	<b>313</b>
Symantec Endpoint Protection Memory Exploit Mitigation techniques.....	317
<b>Ransomware mitigation and protection with Symantec Endpoint Protection.....</b>	<b>319</b>
<b>Ransomware protection using Symantec Endpoint Protection.....</b>	<b>321</b>
<b>Preventing and handling virus and spyware attacks on client computers.....</b>	<b>324</b>
Removing viruses and security risks.....	325
Identifying the infected and at-risk computers.....	327
Checking the scan action and rescanning the identified computers.....	327
How Windows clients receive definitions from the cloud.....	328
Managing scans on client computers.....	330
About the types of scans and real-time protection.....	331
About the types of Auto-Protect.....	333
About virus and security risks.....	335
About the files and folders that Symantec Endpoint Protection excludes from virus and spyware scans.....	336
About the default Virus and Spyware Protection policy scan settings.....	338
How Symantec Endpoint Protection handles detections of viruses and security risks.....	340
How Symantec Endpoint Protection handles detections on Windows 8 computers.....	341
Setting up scheduled scans that run on Windows computers.....	342
Setting up scheduled scans that run on Mac computers.....	343
Setting up scheduled scans that run on Linux computers.....	344
Running on-demand scans on client computers.....	345
Adjusting scans to improve computer performance.....	345
Adjusting scans to increase protection on your client computers.....	347
Managing Download Insight detections.....	349
How Symantec Endpoint Protection uses Symantec Insight to make decisions about files.....	351
How does Symantec Endpoint Protection use advanced machine learning?.....	352

---



---

How does the emulator in Symantec Endpoint Protection detect and clean malware?.....	354
Managing the quarantine for Windows clients.....	355
Managing the virus and spyware notifications that appear on client computers.....	357
About the pop-up notifications that appear on Windows 8 clients.....	358
Enabling or disabling Symantec Endpoint Protection pop-up notifications that appear on Windows 8 clients.....	358
Managing early launch anti-malware (ELAM) detections.....	359
Adjusting the Symantec Endpoint Protection early launch anti-malware (ELAM) options.....	360
Configuring a site to use a private Insight server for reputation queries.....	360
Configuring client groups to use private servers for reputation queries and submissions.....	361
<b>Customizing virus and spyware scans.....</b>	<b>362</b>
Customizing the virus and spyware scans that run on Mac computers.....	364
Customizing the virus and spyware scans that run on Linux computers.....	364
Customizing Auto-Protect for Windows clients.....	365
Customizing Auto-Protect for Mac clients.....	366
Customizing Auto-Protect for Linux clients.....	367
Customizing Auto-Protect for email scans on Windows computers.....	368
Customizing administrator-defined scans for clients that run on Windows computers.....	369
Customizing administrator-defined scans for clients that run on Mac computers.....	370
Customizing administrator-defined scans for clients that run on Linux computers.....	370
Randomizing scans to improve computer performance in virtualized environments on Windows clients.....	371
Modifying global scan settings.....	372
Modifying log handling and notification settings on Windows computers.....	373
Modifying log handling settings on Linux computers.....	373
Customizing Download Insight settings.....	373
Changing the action that Symantec Endpoint Protection takes when it makes a detection.....	374
Allowing users to view scan progress and interact with scans on Windows computers.....	376
Configuring Windows Security Center notifications to work with Symantec Endpoint Protection clients.....	377
<b>Submitting Symantec Endpoint Protection telemetry to improve your security.....</b>	<b>378</b>
Understanding server data collection and client submissions and their importance to the security of your network.....	386
Managing the pseudonymous or non-pseudonymous data that clients send to Symantec.....	388
How Symantec Endpoint Protection minimizes the impact of client submissions on your network bandwidth.....	388
Specifying a proxy server for client submissions and other external communications.....	389
<b>Managing SONAR.....</b>	<b>390</b>
About SONAR.....	391
Handling and preventing SONAR false positive detections.....	392
Adjusting SONAR settings on your client computers.....	393
Monitoring SONAR detection results to check for false positives.....	394
Changing Tamper Protection settings.....	395
<b>About application control, system lockdown, and device control.....</b>	<b>395</b>

---

---

Setting up application control.....	396
Enabling and testing default application rules.....	397
The structure of an Application Control and Device Control policy.....	398
Adding custom rules to Application Control.....	399
Best practices for adding application control rules.....	401
Best practices for choosing which condition to use for a rule.....	402
Testing application control rules.....	403
Configuring system lockdown.....	404
Creating a file fingerprint list with checksum.exe.....	407
Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager.....	409
Manually updating a file fingerprint list in Symantec Endpoint Protection Manager.....	410
Interaction between system lockdown and Symantec EDR deny list (blacklist) rules.....	410
Creating an application name list to import into the system lockdown configuration.....	411
Automatically update file fingerprint lists to allow or block for system lockdown.....	412
Setting up and testing the system lockdown configuration before you enable system lockdown.....	415
Running system lockdown in allow mode.....	416
Running system lockdown in deny mode.....	417
Managing device control.....	418
Allowing or blocking devices on client computers.....	418
About the hardware devices list.....	419
Obtaining a device vendor or model for Windows computers with DevViewer.....	420
Adding a hardware device to the Hardware Devices list.....	421
<b>Managing exceptions in Symantec Endpoint Protection.....</b>	<b>422</b>
Which Windows exceptions do I use for what type of scan?.....	423
Creating exceptions for Virus and Spyware scans.....	424
Excluding a file or a folder from scans.....	426
Excluding known risks from virus and spyware scans on Windows clients.....	427
Excluding file extensions from virus and spyware scans on Windows clients and Linux clients.....	428
Monitoring an application to create an exception for the application on Windows clients.....	428
Specifying how Symantec Endpoint Protection handles monitored applications on Windows clients.....	429
Excluding a trusted web domain from scans on Windows clients.....	429
Creating a Tamper Protection exception on Windows clients.....	430
Creating an exception for an application that makes a DNS or host file change.....	431
Excluding a certificate from scans on Windows clients.....	431
Restricting the types of exceptions that users can configure on client computers.....	432
Creating exceptions from log events.....	432
<b>Configuring Web and Cloud Access Protection.....</b>	<b>433</b>
What is Web and Cloud Access Protection?.....	435
Verifying that the Web and Cloud Access Protection tunnel method is enabled and connected on the client.....	438
Testing Web and Cloud Access Protection policies in a browser.....	440

---

---

About Web and Cloud Access Protection for the Mac client.....	442
Web and Cloud Access Protection Settings.....	442
<b>Testing Symantec Endpoint Protection Manager policies.....</b>	<b>443</b>
Testing a Virus and Spyware Protection policy.....	444
Blocking a process from starting on client computers.....	445
Preventing users from writing to the registry on client computers.....	445
Preventing users from writing to a particular file.....	446
Adding and testing a rule that blocks a DLL.....	447
Adding and testing a rule that terminates a process.....	449
Testing a default IPS policy.....	449
<b>How to update content and definitions on the clients.....</b>	<b>451</b>
Choose a distribution method to update content on clients.....	452
Choose a distribution method to update content on clients based on the platform.....	455
Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager.....	456
Checking that Symantec Endpoint Protection Manager has the latest content.....	459
About the types of content that LiveUpdate downloads.....	460
Configuring clients to download content from an internal LiveUpdate server.....	464
Configuring clients to download content from an external LiveUpdate server.....	465
Configuring Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate.....	466
Specifying a proxy server that clients use to communicate to Symantec LiveUpdate or an internal LiveUpdate server.....	466
Configuring the LiveUpdate download schedule to client computers.....	467
Configuring the amount of control that users have over LiveUpdate.....	469
Mitigating network overloads for client update requests.....	469
About randomization of simultaneous content downloads.....	470
Randomizing content downloads from the default management server or a Group Update Provider.....	470
Randomizing content downloads from a LiveUpdate server.....	471
Configuring Windows client updates to run when client computers are idle.....	472
Configuring Windows client updates to run when definitions are old or the computer has been disconnected.....	472
Configuring clients to download content from the Symantec Endpoint Protection Manager.....	473
Testing engine updates before they release on Windows clients.....	473
Reverting to an older version of the Symantec Endpoint Protection security updates.....	475
Using Group Update Providers to distribute content to clients.....	476
About the types of Group Update Providers.....	477
Configuring clients to download content from Group Update Providers.....	479
Searching for the clients that act as Group Update Providers.....	480
About the effects of configuring more than one type of Group Update Provider in your network.....	481
Using Intelligent Updater files to update content on Symantec Endpoint Protection clients.....	482

---

---

<b>Using third-party distribution tools to update client computers.....</b>	<b>483</b>
Configuring a LiveUpdate Settings policy to allow third-party content distribution to managed clients.....	484
Preparing unmanaged clients to receive updates from third-party distribution tools.....	484
Distributing the content using third-party distribution tools.....	485
<b>Monitoring, Reporting, and Enforcing Compliance.....</b>	<b>488</b>
<b>Setting up Host Integrity.....</b>	<b>488</b>
How Host Integrity works.....	489
About Host Integrity requirements.....	489
Adding predefined requirements to a Host Integrity policy.....	490
Setting up remediation for a predefined Host Integrity requirement.....	491
Allowing users to delay or cancel Host Integrity remediation.....	491
Configuring the frequency of Host Integrity check settings.....	492
Allowing the Host Integrity check to pass if a requirement fails.....	493
Configuring notifications for Host Integrity checks.....	493
Creating a Quarantine policy for a failed Host Integrity check.....	494
Blocking a remote computer by configuring peer-to-peer authentication.....	494
Adding a custom requirement from a template.....	495
Writing a customized requirement script.....	496
About registry conditions.....	497
Writing a custom requirement to run a script on the client.....	498
Writing a custom requirement to set the timestamp of a file.....	498
Writing a custom requirement to increment a registry DWORD value.....	499
Creating a test Host Integrity policy with a custom requirement script.....	500
<b>Monitoring endpoint protection.....</b>	<b>501</b>
Finding unscanned computers.....	503
Finding offline computers.....	504
Generating a list of the Symantec Endpoint Protection versions installed in your network.....	504
Running a report on the deployment status of clients.....	505
Viewing risks.....	505
Viewing attack targets and sources.....	506
Viewing a daily or weekly status report.....	507
Viewing system protection.....	507
<b>Configuring reporting preferences.....</b>	<b>507</b>
<b>Logging on to reporting from a standalone web browser.....</b>	<b>508</b>
<b>About the types of Symantec Endpoint Protection Manager reports.....</b>	<b>509</b>
<b>Running and customizing quick reports.....</b>	<b>516</b>
<b>Saving custom reports.....</b>	<b>517</b>
<b>How to run scheduled reports.....</b>	<b>518</b>
<b>Editing the filter used for a scheduled report.....</b>	<b>519</b>
<b>Printing and saving a copy of a report.....</b>	<b>520</b>

---

---

<b>Viewing logs.....</b>	<b>520</b>
About the types of Symantec Endpoint Protection Manager logs.....	521
Saving and deleting custom logs by using filters.....	523
Viewing logs from other sites.....	524
Exporting data to a Syslog server.....	524
Exporting log data to a text file.....	525
Configuring a failover server for external logging.....	526
<b>Managing notifications.....</b>	<b>527</b>
How notifications work.....	527
What are the types of notifications and when are they sent?.....	528
About partner notifications.....	531
<b>Establishing communication between the management server and email servers.....</b>	<b>531</b>
<b>Viewing and acknowledging notifications.....</b>	<b>531</b>
<b>Saving and deleting administrative notification filters.....</b>	<b>532</b>
<b>Setting up administrator notifications.....</b>	<b>533</b>
<b>How upgrades from another version affect notification conditions.....</b>	<b>534</b>
<b>Managing management servers, sites, and databases.....</b>	<b>536</b>
About the types of Symantec Endpoint Protection servers.....	536
Exporting and importing server settings.....	536
Managing Symantec Endpoint Protection Manager servers and third-party servers.....	537
Maintaining the database.....	538
Running automatic database backups.....	540
Scheduling automatic database maintenance tasks.....	541
Increasing the Microsoft SQL Server database file size.....	542
Specifying client log size and which logs to upload to the management server.....	542
Specifying the log size and how long to keep log entries in the database.....	543
About increasing the disk space on the server for client log data.....	543
Clearing log data from the database manually.....	544
<b>Setting up failover and load balancing.....</b>	<b>544</b>
About failover and load balancing.....	545
Configuring a management server list for load balancing.....	547
Installing a management server for failover or load balancing.....	547
Assigning a management server list to a group and location.....	548
<b>Setting up sites and replication.....</b>	<b>549</b>
What are sites and how does replication work?.....	550
How to resolve data conflicts between sites during replication.....	552
Deciding whether or not to set up multiple sites and replication.....	553
Determining how many sites you need.....	554
How to install a second site for replication.....	555
Changing the replication frequency and content.....	556

---

---

Replicating data immediately.....	557
Deleting sites.....	557
<b>Disaster recovery best practices for Endpoint Protection.....</b>	<b>557</b>
Backing up the database and logs.....	559
Backing up a server certificate.....	560
Reinstalling or reconfiguring Symantec Endpoint Protection Manager.....	560
Generating a new server certificate.....	561
Restoring the database.....	562
<b>Managing clients and policies from the Symantec Endpoint Security cloud console.....</b>	<b>564</b>
What is Symantec Endpoint Security (SES) and the Integrated Cyber Defense Manager (ICDm) cloud console?.....	564
Choosing between the on-premises management, hybrid management, or cloud-only management options.....	565
Enrolling a Symantec Endpoint Protection Manager domain into the cloud console.....	567
What happens after you enroll a Symantec Endpoint Protection Manager domain into the cloud console?.....	570
How a hybrid-managed Symantec Endpoint Protection Manager interacts with the Symantec Endpoint Security cloud console.....	571
How 14.x Symantec Endpoint Protection Manager domain-enrolled cloud console features compare to on-premises Symantec Endpoint Protection Manager.....	574
How does the Symantec Endpoint Protection Manager Exceptions policy interact with the cloud console?.....	577
Enrolling sites with replication partners in the cloud console.....	580
Updating clients in low-bandwidth environments.....	582
Unenrolling Symantec Endpoint Protection Manager domains from the cloud console.....	583
<b>Using Symantec Endpoint Protection in virtual infrastructures.....</b>	<b>585</b>
About Shared Insight Cache.....	585
About the Virtual Image Exception tool.....	586
What do I need to do to use a network-based Shared Insight Cache?.....	586
System requirements for implementing a network-based Shared Insight Cache.....	587
Installing and uninstalling a network-based Shared Insight Cache.....	587
Enabling the use of a network-based Shared Insight Cache.....	588
Customizing Shared Insight Cache settings.....	589
About stopping and starting the network-based Shared Insight Cache service.....	592
Viewing network-based Shared Insight Cache log events.....	592
Monitoring network-based Shared Insight Cache performance counters.....	593
Troubleshooting issues with Shared Insight Cache.....	593
Using the Virtual Image Exception tool on a base image.....	594
System requirements for the Virtual Image Exception tool.....	594
Running the Virtual Image Exception tool.....	595
Configuring Symantec Endpoint Protection to bypass the scanning of base image files.....	595
<b>Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures.....</b>	<b>596</b>

---

---

Setting up the base image for non-persistent guest virtual machines in VDIs.....	596
Purging obsolete non-persistent VDI clients to free up licenses.....	597
How to manage the license count for non-persistent VDI clients.....	597
viptool.....	598
viptool.....	598
<b>Troubleshooting Symantec Endpoint Protection.....</b>	<b>599</b>
URLs that allow (whitelist) SEP and SES to connect to Symantec servers.....	600
Troubleshooting computer issues with the Symantec Diagnostic Tool (SymDiag).....	600
Identifying the point of failure of a client installation.....	600
Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client.....	601
Checking the connection to the management server on the client computer.....	602
Investigating protection problems using the troubleshooting file on the client.....	602
Enabling and viewing the Access log to check whether the client connects to the management server.....	602
Stopping and starting the Apache Web server.....	603
Using the ping command to test the connectivity to the management server.....	603
Using a browser to test the connectivity to Symantec Endpoint Protection Manager on the Symantec Endpoint Protection client.....	603
Checking the debug log on the client computer.....	604
Checking the inbox logs on the management server.....	604
Restoring client-server communication settings by using the SymlinkDrop tool.....	605
Troubleshooting the Symantec Linux Agent.....	606
Troubleshooting communication problems between Symantec Endpoint Protection Manager and the console or the default database.....	607
Verifying the management server connection with the database.....	607
Client and server communication files.....	610
Troubleshooting reporting issues.....	610
Changing timeout parameters for reviewing reports and logs.....	611
Accessing reporting pages when the use of loopback addresses is disabled.....	612
What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console.....	613
Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console.....	615
Starting Power Eraser analysis from Symantec Endpoint Protection Manager.....	617
Responding to Power Eraser detections.....	618
<b>Appendices.....</b>	<b>620</b>
Symantec Endpoint Protection features based on platform.....	620
Symantec Endpoint Protection feature dependencies for Windows clients.....	629
What are the tools included with Symantec Endpoint Protection?.....	631
Commands for the Windows client service smc in Symantec Endpoint Protection and Symantec Endpoint Security.....	637

---



<b>smc.exe command error codes.....</b>	<b>642</b>
<b>Installing Windows client software using third-party tools.....</b>	<b>643</b>
<b>About client installation features and properties.....</b>	<b>644</b>
About configuring MSI command strings.....	644
About configuring Setaid.ini.....	644
<b>Symantec Endpoint Protection command-line client installation properties.....</b>	<b>645</b>
<b>Installing Symantec Endpoint Protection client features using the command line.....</b>	<b>646</b>
<b>Windows Installer parameters.....</b>	<b>647</b>
<b>Windows Security Center properties.....</b>	<b>648</b>
<b>Command-line examples for installing the Windows client.....</b>	<b>649</b>
<b>Installing Windows clients with Microsoft SCCM/SMS.....</b>	<b>649</b>
<b>Installing Windows clients with an Active Directory Group Policy Object (GPO).....</b>	<b>650</b>
Creating a GPO software distribution.....	651
Adding computers to an organizational unit to install software.....	652
Copying a Sylink.xml file to make a managed installation package.....	653
<b>Uninstalling client software with an Active Directory Group Policy Object.....</b>	<b>654</b>
<b>Quick Start Guide for Symantec™ Endpoint Protection for Amazon Web Services.....</b>	<b>654</b>
<b>What's new for Symantec Endpoint Protection (SEP) 14.0.1 (14 RU1).....</b>	<b>656</b>
<b>What's new in Symantec Endpoint Protection (SEP) 14.....</b>	<b>659</b>
<b>Glossary.....</b>	<b>667</b>
Bloodhound.....	667
Early Launch Anti-Malware.....	667
File Reputation.....	667
Insight.....	667
Insight Lookup.....	667
What is an .slf file?.....	668
Risk Categories.....	668
What is Shared Insight Cache?.....	668
SONAR.....	668
What is Virtual Image Exception?.....	668
<b>Product Dialog Help.....</b>	<b>670</b>
<b>Logs.....</b>	<b>670</b>
Basic filter settings for all logs and quick reports.....	670
Basic options for all logs.....	670
Common additional filter settings for all logs and quick reports.....	670
Audit log and quick reports.....	672
Compliance log and quick report.....	672
Application and Device Control logs and quick reports.....	673
Computer Status logs and reports.....	675



---

Deception logs and reports.....	676
Network and Host Exploit Mitigation logs and quick reports.....	677
SONAR logs.....	678
Risk logs and quick reports.....	680
Scan logs and quick reports.....	683
System logs and quick reports.....	685
Monitors: Summary tab.....	686
Client Log Settings for group name.....	688
Choose Power Eraser Type.....	689
<b>Site/Server Properties.....</b>	<b>690</b>
Site Properties: LiveUpdate.....	690
Download LiveUpdate Content.....	690
Languages to Download.....	691
LiveUpdate Servers.....	691
Add or Edit LiveUpdate Server.....	691
Platforms to Download.....	692
Download Schedule.....	692
Full Definitions Download.....	692
Content to Download for Client Types.....	693
<b>Policies.....</b>	<b>693</b>
Overview.....	693
Policy Components.....	694
Policies.....	695
Withdraw the type of Policy.....	696
Replace the policy.....	696
Search for Applications.....	696
View Details.....	698
<b>Exceptions Policy.....</b>	<b>698</b>
Exceptions.....	699
Exceptions: Client Restrictions.....	699
Application to Monitor.....	699
Application Exception.....	700
Application Exception by Fingerprint.....	701
Known Security Risks Exceptions.....	702
Folder Exception.....	702
File Access Exception.....	703
File Exception.....	704
File and Folder Prefix Variables.....	704
Security Risk Extension Exceptions.....	706
Security Risk File or Folder Exception for Mac clients.....	706

---

---

Trusted Web Domain Exception.....	706
Tamper Protection Exception.....	707
DNS or Host File Change Exception.....	708
Add Folder Exception for Linux clients.....	709
Add Certificate Exception.....	710
<b>LiveUpdate Settings Policy.....</b>	<b>711</b>
LiveUpdate Server Settings for Windows clients.....	711
LiveUpdate Settings Policy: Windows Schedule.....	713
LiveUpdate Settings Policy - Advanced Settings.....	714
Group Update Provider.....	715
Group Update Provider List.....	716
Specify Group Update Provider Rule Criteria.....	717
Configure Explicit Group Update Providers.....	717
Add Explicit Group Update Provider.....	717
IP Address or Host Name.....	719
Registry Keys.....	719
Operating Systems.....	720
Proxy server settings for external communications.....	720
LiveUpdate Server Settings for Mac clients.....	721
LiveUpdate Advanced Server Settings.....	722
LiveUpdate Policy: Mac Schedule.....	722
LiveUpdate Policy Settings Mac Advanced Settings.....	722
HTTP or HTTPS Proxy server settings.....	723
FTP Proxy server settings.....	724
LiveUpdate Server Settings for Linux clients.....	724
LiveUpdate Advanced Server Settings for Linux clients.....	724
Proxy Server Settings for Linux clients.....	725
LiveUpdate Policy: Linux Schedule.....	725
<b>LiveUpdate Content Policy.....</b>	<b>726</b>
Security Definitions.....	726
LiveUpdate Content product updates.....	726
LiveUpdate Content Policy Settings for group name.....	726
Select revision.....	726
Replace LiveUpdate Content policy.....	727
Select an engine version.....	727
<b>Admin page.....</b>	<b>727</b>
License Renewal.....	727
License Main Page.....	728
Upgrade license help.....	728
.....	<b>728</b>

---

---

Clients: Clients.....	728
Clients: Policies.....	732
Clients: Details.....	733
Install Packages.....	734
Select Scan Type.....	734
Add Group for group name.....	734
Add Computer for group name.....	735
Add User for group name.....	735
Integrate with Organizational Unit Tree.....	735
Search Clients.....	736
Export Communications Settings for group name.....	736
Group Properties.....	737
Set Display Filter.....	738
Add Unmanaged Detector Exception.....	738
Unmanaged Detector Exceptions.....	738
<b>Import LDAP Users.....</b>	<b>739</b>
Clients: Properties.....	739
<b>Management server lists.....</b>	<b>742</b>
Add Management Server.....	742
Management server list name: Assigned Groups and Locations.....	742
Management Server Lists.....	742
Replace Management Server List.....	743
Apply Management Server List.....	743
<b>Clients Page &gt; Policies tab.....</b>	<b>744</b>
Communications Settings for <group_name>.....	744
General Settings for group name: General Settings.....	746
General Settings for group name: Security Settings.....	746
Password Settings.....	747
Client User Interface Control Settings for <group name>.....	748
Client User Interface Mixed Control Settings: Client/Server Control Settings.....	749
Client User Interface Settings.....	752
Specify Location Criteria.....	755
Address.....	757
Manage Locations.....	757
Select Restart Options.....	758
Cloud Settings.....	760
<b>Client Submissions.....</b>	<b>760</b>
<b>Tamper Protection.....</b>	<b>761</b>
<b>Administrators and authentication.....</b>	<b>762</b>
Admin Page: Administrators.....	762

---

---

Change password.....	763
Rename Administrator.....	763
Administrator Properties: General.....	763
Administrator properties: <b>Access Rights</b> .....	764
Administrator: Authentication.....	765
Group Rights.....	767
Reporting Rights.....	767
Command Rights.....	767
Policy Rights.....	768
Site Rights.....	768
<b>Domains.....</b>	<b>769</b>
Admin Page: Domains.....	769
Add Domain.....	769
Edit Domain Properties: General.....	770
Edit Domain Properties: Logon Banner.....	771
Domain Properties: Passwords.....	772
<b>Servers and Databases.....</b>	<b>772</b>
Servers.....	772
Management Server.....	772
Deny/Allow Console Access.....	772
Test Configuration.....	773
Edit IP Addresses.....	773
Server Properties: General.....	773
Server Properties: Email Server.....	774
Server Properties: Directory Servers.....	774
Server Properties: Proxy Server.....	775
Server Properties: File Fingerprint Update.....	776
Add Directory Server: General.....	777
Add Directory Server: Replication Servers.....	778
Database Server.....	778
Database Properties: General.....	778
Database Properties: Log Settings.....	778
Database Properties: Backup Settings.....	779
Truncate Database Transaction Log.....	780
Rebuild Indexes.....	780
Add Certificate.....	780
Configure Symantec VIP Authentication.....	780
Configure Smart Card Authentication.....	781
<b>Site properties and replication.....</b>	<b>781</b>
Local Site.....	781

---

---

Site Properties: General.....	782
Site Properties: Passwords.....	783
Site Properties: Data Collection.....	783
Site Properties: Private Insight Server.....	783
External Logging for site name: Log Filter.....	784
External Logging for site name: General.....	784
Replication Partners.....	785
Replication Partner Properties.....	785
Replication Partner Properties for a Site.....	785
Remote Sites Management.....	786
<b>Management Server Configuration Wizard.....</b>	<b>786</b>
Management Server Configuration.....	786
Creating the system administrator account and configuring the email server.....	786
Selecting a configuration type.....	788
Selecting the type of database to use.....	789
About creating an encryption password.....	790
Specifying the database password during server reconfiguration.....	791
Installing a new site as a replication partner to an existing site.....	791
<b>Installation Packages.....</b>	<b>792</b>
Client Install Packages: Overview.....	792
Client Install Settings: Overview.....	792
Client Install Feature Set: Overview.....	792
Client Install Settings.....	792
Client Install Feature Set.....	796
Add a Client Install Package.....	797
Export Package settings.....	798
Client Install Package Properties.....	800
Management Server List for list name.....	800
Add Client Install Package: General.....	800
Set User Information Collection.....	802
Add Client Install Package: Notification.....	802
Client Install Settings for Mac.....	803
<b>Monitoring and Reports.....</b>	<b>805</b>
Home page.....	805
Preferences: Home page and Monitors page.....	807
Preferences: Security Status.....	808
Preferences: Logs and Reports.....	808
Command Status.....	809
Command Status: Details.....	810
Scheduled Reports.....	811

---

---

Scheduled Reports: Add Scheduled Report or Edit Scheduled Report.....	812
Scheduled Reports: Edit Filter.....	813
<b>Virus and Spyware Protection.....</b>	<b>813</b>
Auto-Protect: Notifications.....	813
Internet Email Auto-Protect: Notifications.....	814
Microsoft Outlook or Lotus Notes Auto-Protect: Notifications.....	815
Rules: Notifications.....	816
Monitors: Notifications.....	817
Add or Edit Notification Condition.....	818
Notification Conditions.....	822
Global Scan Options: Scan Network Drive: Change password.....	823
Miscellaneous.....	823
Miscellaneous: Log handling.....	824
Miscellaneous: Notifications.....	825
Customize Error Message.....	826
Auto-Protect for Microsoft Outlook, Internet Email, or Lotus Notes: Actions.....	826
Floppy Settings.....	828
Network Settings.....	828
Auto-Protect: Advanced.....	829
Internet Email Auto-Protect: Scan Details.....	829
Insert Warning.....	830
Email Server.....	832
Message.....	832
Send Email to Others: Others.....	833
Internet Email Auto-Protect: Advanced.....	833
Microsoft Outlook Auto-Protect: Scan Details.....	835
Lotus Notes Auto-Protect: Scan Details.....	836
Outdated Virus Definitions Warning.....	837
Absent Virus Definitions Warning.....	837
Administrator-defined Scans: Scans.....	837
Add Scheduled Scan.....	838
Scan Details.....	838
Advanced Scanning Options: Compressed Files.....	839
Advanced Scanning Options: Storage Migration.....	840
Advanced Scanning Options: Tuning.....	841
Scheduled Scan: Schedule.....	842
Administrator-defined Scans: Advanced.....	844
Scan Pause Options.....	846
Quarantine: Cleanup.....	846
Common Settings for Mac client scans.....	846

---

---

Mac Auto-Protect and SONAR: Scan Details.....	847
Legacy client settings: Scan Mounted Disk Details (Mac only).....	848
On-demand scan details for Mac clients.....	848
Mac Global Scan Options.....	849
Mac Global Scan Options: Files and folders to scan.....	849
Download Protection: Download Insight.....	850
Download Protection: Actions.....	852
Download Protection: Notifications.....	853
Global Scan Options.....	854
Edit Folders.....	854
File Extensions.....	855
Risk Tracer.....	857
File Cache.....	858
Auto-Protect: Scan Details.....	859
Advanced Scanning and Monitoring.....	861
Quarantine: General.....	863
Scheduled scan details for Mac clients.....	864
Administrator-defined Scans: Notifications.....	864
Early Launch Anti-Malware Driver Options.....	865
Actions.....	866
Edit scheduled scan: Scan details.....	868
Linux Global Scan Options.....	868
Linux Auto-Protect: Advanced Scanning and Monitoring.....	869
Linux Auto-Protect: Scan Details.....	869
Linux Auto-Protect: Advanced.....	870
Custom Process List.....	871
SONAR: SONAR.....	871
<b>Application Control and Device Control.....</b>	<b>873</b>
System Lockdown for group name.....	873
Unapproved Applications.....	875
Add File or Folder Definition.....	875
Application Control: Application Control Rule Sets.....	875
Add Application Control Rule Set.....	876
Registry Access Attempts properties.....	877
Add Registry Key Definition.....	877
Registry Access or File and Folder Access Attempts: Actions tab.....	878
File and Folder Access Attempts properties.....	878
Launch or Terminate Process Attempts properties.....	879
Add Process Definition.....	879
Launch Process, Terminate Process, or Load DLL Attempts: Actions tab.....	881

---

---

Load DLL Attempts properties.....	882
Add DLL Definition.....	882
Device Control.....	883
Mac Device Control in Endpoint Protection 14.....	884
Add Notification Message.....	886
Hardware Device.....	886
<b>Firewall Policy.....</b>	<b>887</b>
Rules: Rules.....	887
Application List.....	889
Add Application.....	889
Network Adapter.....	889
Windows Integration.....	890
Network Adapter.....	890
Select Host.....	891
Add or Edit Host.....	893
Host Groups.....	894
Schedule List.....	894
Add Schedule.....	894
Service List.....	895
Protocol.....	895
Network Service.....	898
Built-in Rules.....	899
Protection and Stealth Settings.....	900
Peer-to-Peer Authentication Settings.....	902
Network Application Monitoring for <group name>.....	903
<b>Intrusion Prevention System Policy.....</b>	<b>903</b>
Excluded Hosts.....	903
Exceptions.....	904
Intrusion Prevention settings.....	904
Add Intrusion Prevention Exceptions.....	906
Signature Action.....	906
Custom Intrusion Prevention Signatures: Signatures.....	907
Intrusion Prevention Signature Group.....	908
Add Application or Edit Application.....	908
Custom Intrusion Prevention Signatures: Variables.....	908
Add Variable or Edit Variable.....	909
Custom Intrusion Prevention for Group name.....	909
Add Signature or Edit Signature.....	909
Regular expressions in custom IPS signature content and application control rules.....	910
<b>Syntax for custom intrusion prevention signatures.....</b>	<b>913</b>

---



---

<b>Memory Exploit Mitigation Settings.....</b>	<b>921</b>
Memory Exploit Mitigation.....	923
<b>Host Integrity Policy.....</b>	<b>923</b>
Requirements.....	923
Add Requirement.....	923
Advanced Settings.....	923
Custom requirement: Select a condition.....	924
Custom requirement.....	925
Custom Requirement: Customized Requirement Script.....	926
Add Requirement: Antivirus requirement.....	926
Add Requirement: Antispyware requirement.....	927
Add Requirement: Patch.....	928
Add Requirement: Service pack.....	929
Add Requirement: Firewall requirement.....	930
About specifying the file location and execute command for remediation.....	931
Antivirus: Antivirus is installed.....	931
Antivirus: Antivirus is running.....	931
Antivirus: Antivirus signature file is up-to-date.....	931
Antispyware: Antispyware is installed.....	932
Antispyware: Antispyware is running.....	932
Antispyware: Antispyware signature file is up-to-date.....	932
Antivirus: Check not infected.....	932
Firewall: Firewall is installed.....	932
Firewall: Firewall is running.....	932
Patch: Compare current service pack with specified version.....	932
Patch: Patch is installed.....	933
File: Compare file age to.....	933
File: Compare file date to.....	933
File: Compare file size to.....	933
File: Compare file version to.....	933
File: File download complete.....	933
File: File exists.....	934
File: File fingerprint equals.....	934
Registry: Registry key exists.....	934
Registry: Registry value exists.....	934
Registry: Registry value equals.....	935
Registry: Set registry value.....	935
Registry: Set registry value successful.....	935
Registry: Increment registry DWORD value.....	936
Utility: Check timestamp.....	936

---

---

Utility: Message dialog return value equals true.....	936
Utility: Operating system is.....	936
Utility: Operating system language is.....	936
Utility: Process is running.....	936
Utility: Service is running.....	937
File: Download a file.....	937
Utility: Log message.....	937
Utility: Run a program.....	937
Utility: Run a script.....	938
Utility: Set timestamp.....	938
Utility: Show message dialog.....	938
Utility: Wait.....	938
<b>Miscellaneous: Virtual Images.....</b>	<b>938</b>
Miscellaneous: Shared Insight Cache.....	939
Change Password.....	940
<b>Private Cloud.....</b>	<b>940</b>
Copy private server settings.....	941
Private Cloud: Add or Edit Private Server.....	941
<b>Cloud: Overview.....</b>	<b>941</b>
<b>Related Documents.....</b>	<b>943</b>
<b>Copyright statement.....</b>	<b>944</b>

---

## Release Notes

---

Includes the system requirements, supported upgrade paths, known issues, and links to more information

Review the release notes before you install or upgrade Symantec Endpoint Protection, or contact Technical Support. The release notes include installation changes, upgrade issues, and known issues and workarounds.

### What's new for Symantec Endpoint Protection 14.3 RU2?

This section describes the new features in this release.

#### Protection Features

- Includes runtime protection against fileless threats such as malicious Excel macros (XLM) and payloads using Windows Management Instrumentation (WMI) with our expanded integration with Antimalware Scan Interface (AMSI).
- Enhanced behavior detection and prevention protects against ransomware families such as Ryuk and Netwalker with improved behavioral detection and prevention of malicious modification or removal of user files.
- Enhancements have been made to the emulator in the Symantec Endpoint Protection client to increase detection of cryptocurrency mining malware families like LemonDuck.
- A **browser extension** provides better protection for both HTTP and HTTPS traffic to and from the Google Chrome web browser. The Symantec Endpoint Protection client blocks users from accessing malicious sites and redirects users to a default landing page. The browser extension depends on IPS; therefore, the IPS policy must be enabled and assigned to the group. The browser extension is downloaded from LiveUpdate by default if the computer joined an Active Directory domain. Otherwise, the browser extension is downloaded from the Google Web Store. You enable or disable this content by clicking **Admin > Servers > Edit Site Properties > LiveUpdate tab > Content Types to Download > Browser Extension**.

By default, the Symantec Endpoint Protection installer installs the Google Chrome browser extension. However, if you want to use an Active Directory Group Policy Object to manage your Chrome extensions, you must add the browser extension to your list. See:

[Integrating browser extensions with Symantec Endpoint Protection to protect against malicious websites](#)

[Installing the Endpoint Protection Chrome Browser Extension using Group Policy Object](#)

[About the types of content that LiveUpdate downloads](#)

- Ability for administrators to retrieve quarantined files on remote SEP clients from the Symantec Endpoint Protection Manager console. These malicious files can be used for further investigating and sandboxing. To upload the quarantined file, check the **Admin > Domains > Edit Domain Properties > General tab > Upload quarantined files from the clients** option. This option automatically uploads all quarantined files from the clients. You can then select and retrieve individual files from the Risk log using the **Download file that the client quarantined** command. The management server no longer supports old versions of the Central Quarantine Server, so the Virus and Spyware Protection policy > **Quarantine > Quarantined Items** options were removed.

[Managing the quarantine for Windows clients](#)

- Intrusion Prevention (IPS) content has been optimized considerably to reduce content size and improve network throughput. This improvement is available to all supported Symantec Endpoint Protection versions.
- Network Traffic Redirection is renamed to Web and Cloud Access Protection in the Symantec Endpoint Protection Manager, Windows client, and Mac client. In the client, users can click a **Reconnect** button in the **Web and Cloud Access Protection > Options** menu. Client users should use this option if the client does not detect that the connection with the Symantec WSS has been broken.

[Configuring Web and Cloud Access Protection](#)

#### Symantec Endpoint Protection Manager

- Includes automatic LiveUpdate for critical fixes and security updates. Starting with SEP 14.3 RU2, critical patches and security fixes are delivered automatically to clients via LiveUpdate to reduce the administrative burden of managing agent updates. These patches include critical fixes only; new features are delivered separately via Release Updates (RUs). To make sure that client patches and client product updates are downloaded from a LiveUpdate server to the Symantec Endpoint Protection Manager, go to the Site properties and select **Client patches** and **Client product updates**. These options are enabled by default.

#### Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager

- To download client patches from the Symantec Endpoint Protection Manager to the clients, in the LiveUpdate Settings policy, click **Advanced Settings > Download client patches**. The LiveUpdate policy downloads the client patch to the client like any other content; the client patch is an incremental delta file.

#### Installing Endpoint Protection client patches on Windows clients

- To download product updates, select **Download delta content from a LiveUpdate server when available**. The client tries to get a smaller amount of content from LiveUpdate if Symantec Endpoint Protection Manager only has full content. Use this option if you not want to enable client patches. The product updates option then ensures that patch builds are available in AutoUpgrade. LiveUpdate downloads a full client installation package to the management server, where the package appears in the **Admin > Install Packages > Client Install Package** table and in the AutoUpgrade wizard. This option is enabled by default. The version of the client does not change, only the build number. Use this option so that the client receives a smaller content from LiveUpdate if management server only has full content.

#### Upgrading client software with AutoUpgrade

- In earlier releases, these options were **Download client security patches** and **Download client patches smaller content from a LiveUpdate server when available**. The **Site Properties > LiveUpdate tab > Content Types to Download > Client patches** option was **Client security patches**.
- The Management Server Configuration Wizard no longer prompts you for credentials to check whether or not the SQL Server FILESTREAM is enabled. Upgrades from an embedded database (14.3 and earlier) automatically enables FILESTREAM. Upgrades from 14.3 RU1/RU1 MP1 keep the existing FILESTREAM setting. The wizard prompts for credentials only if FILESTREAM is not already enabled on the SQL Server Express database.

#### Enabling FILESTREAM for the Microsoft SQL Server database

- Both the Symantec Endpoint Protection clients and the Symantec Endpoint Protection Manager is localized in the following five languages only: English, French, Spanish, Portuguese, and Japanese. If you are using one of the five supported languages, no action is required; you can upgrade as usual. You can automatically upgrade the client language to English if the previous clients' language is unavailable. If you do not choose English, the clients with an unsupported language do not get upgraded. This option is off by default. To enable this option, click **Clients** page > **Install Packages** page, click **Add a Client Install Package > Upgrade to English if unsupported language is unavailable**. This option applies to the Windows client only.

#### Upgrading Symantec Endpoint Protection 14.3 RU2+ to a supported language

- Location awareness has four new criteria: the computer's host name, user and group name, operating system, and whether a particular file runs on the client.

#### Adding a location to a group

- Added additional permission levels for accessing the SEPM REST APIs. Previously, only system administrators could perform any sort of POST operations. Now, domain administrators and limited administrators can monitor the health of their computers using the API. SOC analysts can use third-party tools to integrate with the API. The following APIs have been updated to support role-based access to the API.

HTTP method	Path	Description
POST	/api/v1/identity/authenticate	Authenticates and returns a
POST	/api/v1/identity/logout	Logs off the user that is ass
GET	/api/v1/licenses	Retrieves all license-related
GET	/api/v1/replication/is_replicated	Checks whether a site has a

POST	/api/v1/replication/replicatenow	Initiates replication for the s
GET	/api/v1/replication/status	Gets the replication status.
POST	/api/v1/reporting/authenticate	Authenticates and return a l
GET	/api/v1/sessions/currentuser	Gets the current user token
GET	/api/v1/version	Gets the current version of s

- On the **Admin** page > **Administrators** > **Access Rights** tab, the **Allow editing of shared policies** command was changed from **Do not allow editing of shared policies**. The **Do not allow editing of shared policies** checkbox was not selected by default, which causes administrators to explicitly grant permissions, rather than explicitly deny permissions.
- The following third-party components were upgraded or added: Apache Commons FileUpload, jQuery, PHP with zip extensions enabled, Microsoft Drivers for PHP for Microsoft SQL Server, and OpenSSL.
- The DeVViewer tool is no longer installed with Symantec Endpoint Protection Manager in the Tools\DevViewer folder. Instead, download DevViewer to the client computer from the Attachments section at: [Use DevViewer to find hardware device IDs for Device Blocking in Endpoint Protection](#). You use the DevViewer to obtain the device vendor, model, or serial number of a specific device so that you can allow or block the device in the Device Control policy.

## Client and platform updates

Windows client:

- The Symantec Endpoint Protection client for Windows client supports Citrix Studio Version 2009.0.0, Nutanix AOS 5.15 (LTS), and VMware ESXi 7.0 Update 2.

Mac client:

### NOTE

Symantec Endpoint Protection Manager 14.3 RU2 ships with the last release of the Symantec Endpoint Protection client for Mac 14.3 RU1 MP1. When the Mac client 14.3 RU2 is available, LiveUpdate downloads the Mac client installation package to the Symantec Endpoint Protection Manager **Admin > Install Packages > Client Install Package** page. If you add a **New software package** notification to the **Monitors** page, you receive a notification when the installation package is ready. This feature allows you to upgrade to the latest Symantec Endpoint Protection Manager sooner.

- Supported on devices with the Apple M1 chip.
- AppleScript integration with the Mac client lets you create and run AppleScript scripts to query or control your Mac client.  
[Checking on your Mac client using AppleScript scripts](#)
- The Mac client installation package contains a tool that lets you remove the NLOK build of the Mac client (version 14.3 and earlier) from your Mac device and silently upgrade to a later version of Mac client.
- Performance improvements on the Mac client include: highly enhanced network throughput when using Mac client; performance improvement of Quick Scan; a smaller size of the client installer; and optimized CPU and memory usage.
- Support for the Evidence of Compromise search and the Quarantine File command for remediation. These features are supported on the clients that are managed by the Symantec Endpoint Security cloud console or by the Symantec EDR as of version 4.6.5.

Linux client:

- The Symantec Endpoint Protection client for Linux supports Debian 9 and Debian 10.
- The Symantec Endpoint Protection client for Linux command line tool (sav) lets you control and check on your Linux client.  
[Importing client-server communication settings into the Linux client](#)

## Features Removed

- Extended Support Life for 12.1.x ended on April 3rd 2021.  
[End of Support Life for Endpoint Protection 12.1](#)
- The management server no longer supports old versions of the Central Quarantine Server. The options in the Virus and Spyware Protection policy > **Quarantine > Quarantined Items** page were removed.
- The options in the LiveUpdate policy > **Mac Settings > Advanced Settings** page were removed.
- The **Coexist with Windows Defender** option in the Virus and Spyware Protection policy > **Miscellaneous** page was removed.

#### Documentation

- The Windows client Help files were converted to HTML5 files, which display an updated format and the Broadcom colors.
- You can download PDF files of the release notes for every release on the following page:  
[Related Documents](#)

#### Database schema

The database schema has the following changes.

Table	Column change
HPP_APPLICATION	Added the NONPE column.
Added a new table, REQUESTED_FILES	Added the following columns: <ul style="list-style-type: none"> <li>ID</li> <li>APP_HASH</li> <li>COMMAND_ID</li> <li>BINARY_FILE_ID</li> <li>TIME_STAMP</li> <li>USN</li> <li>RETRY_COUNT</li> <li>DELETED</li> </ul>

[What's new in all releases of Symantec Endpoint Protection](#)

## System requirements for Symantec Endpoint Protection (SEP) 14.3 RU3

In general, the system requirements for the following are the same as those of the operating systems on which they are supported.

#### NOTE

An earlier version of Symantec Endpoint Protection Manager may not be able to correctly manage a client with a later version. Issues with content updates and client management may occur. For example, Symantec Endpoint Protection Manager 14.0.1 or earlier cannot correctly provide a version 14.2 client with its version-specific monikers. Symantec Endpoint Protection Manager for versions earlier than 14 MP2 cannot correctly provide client versions later than 14.0.1 with their version-specific monikers.

The following tables describe the software and hardware requirements for Symantec Endpoint Protection.

**Table 1: Symantec Endpoint Protection Manager (SEPM) software system requirements**

Component	Requirements
Operating system	<ul style="list-style-type: none"> <li>Windows Server 2008 R2</li> <li>Windows Server 2012</li> <li>Windows Server 2012 R2</li> <li>Windows Server 2016</li> <li>Windows Server 2019</li> <li>Windows Server 2022</li> </ul> <p><b>Note:</b> Desktop operating systems are not supported.</p> <p><b>Note:</b> Windows Server Core edition is not supported on 14.2x and earlier.</p>
Web browser	<p>The following browsers are supported for web console access to Symantec Endpoint Protection Manager and for viewing the Symantec Endpoint Protection Manager Help:</p> <ul style="list-style-type: none"> <li>Microsoft Edge Chromium Based Browser (14.3 and later)</li> <li>Microsoft Edge</li> </ul> <p>Note: The 32-bit version Windows 10 does not support web console access on the Edge browser.</p> <ul style="list-style-type: none"> <li>Microsoft Internet Explorer 11 (14.2.x and earlier)</li> <li>Mozilla Firefox 5.x through 83</li> <li>Google Chrome 87</li> </ul>
Database	<p>The Symantec Endpoint Protection Manager includes a default database:</p> <ul style="list-style-type: none"> <li>Microsoft SQL Server Express 2014 (for Windows Server 2008 R2)</li> <li>Microsoft SQL Server Express 2017</li> <li>Sybase embedded database (14.3 MP.x and earlier only)</li> </ul> <p>You may instead choose to use a database from one of the following versions of Microsoft SQL Server:</p> <ul style="list-style-type: none"> <li>SQL Server 2008 SP4</li> <li>SQL Server 2008 R2, SP3</li> <li>SQL Server 2012 RTM - SP4</li> <li>SQL Server 2014 RTM - SP3</li> <li>SQL Server 2016 SP1, SP2</li> <li>SQL Server 2017 RTM</li> <li>SQL Server 2019 RTM (14.3 and later)</li> </ul> <p><b>Note:</b> SQL Server databases that are hosted on Amazon RDS are supported. (14.0.1 MP2 and later).</p> <p><b>Note:</b> If Symantec Endpoint Protection uses a SQL Server database and your environment only uses TLS 1.2, ensure that SQL Server supports TLS 1.2. You may need to patch SQL Server. This recommendation applies to SQL Server 2008, 2012, and 2014.</p> <p><b>Note:</b> <a href="#">TLS 1.2 support for Microsoft SQL Server</a></p>
Other environmental requirements	<ul style="list-style-type: none"> <li>In purely IPv6 networks, the IPv4 stack must still be installed and disabled. If the IPv4 stack is uninstalled, Symantec Endpoint Protection Manager does not work.</li> <li>Microsoft Visual C++ 2017 Redistributable Package (x64/x86)</li> </ul> <p>Note that the required version of Visual C++ is automatically installed during the installation of Symantec Endpoint Protection Manager</p>

**Table 2: Symantec Endpoint Protection Manager hardware system requirements**

Component	Requirements
Processor	Intel Pentium Dual-Core or equivalent minimum, 8-core or greater recommended <b>Note:</b> Intel Itanium IA-64 processors are not supported.
Physical RAM	2 GB RAM available minimum; 8 GB or more available recommended <b>Note:</b> Your Symantec Endpoint Protection Manager server may require additional RAM depending on the RAM requirements of other applications that are already installed. For example, if Microsoft SQL Server is installed on the Symantec Endpoint Protection Manager server, the server should have a minimum of 8 GB available.
Display	1024 x 768 or larger
Hard drive when installing to the system drive	With a local SQL Server database: <ul style="list-style-type: none"><li>• 40 GB available minimum (200 GB recommended) for the management server and database</li></ul> With a remote SQL Server database: <ul style="list-style-type: none"><li>• 40 GB available minimum (100 GB recommended) for the management server</li><li>• Additional available disk space on the remote server for the database</li></ul>
Hard drive when installing to an alternate drive	With a local SQL Server database: <ul style="list-style-type: none"><li>• The system drive requires 15 GB available minimum (100 GB recommended)</li><li>• The installation drive requires 25 GB available minimum (100 GB recommended)</li></ul> With a remote SQL Server database: <ul style="list-style-type: none"><li>• The system drive requires 15 GB available minimum (100 GB recommended)</li><li>• The installation drive requires 25 GB available minimum (100 GB recommended)</li><li>• Additional available disk space on the remote server for the database</li></ul>
Other	An enabled network interface card

If you use a SQL Server database, you may need to make more disk space available. The amount and location of additional space depends on which drive SQL Server uses, database maintenance requirements, and other database settings.



**Table 3: Symantec Endpoint Protection client for Windows software system requirements**

Component	Requirements
Operating system (desktop)	<ul style="list-style-type: none"><li>• Windows 7 (32-bit, 64-bit; RTM and SP1)</li><li>• Windows Embedded 7 Standard, POSReady, and Enterprise (32-bit and 64-bit)</li><li>• Windows 8 (32-bit, 64-bit)</li><li>• Windows Embedded 8 Standard (32-bit and 64-bit)</li><li>• Windows 8.1 (32-bit, 64-bit), including Windows To Go</li><li>• Windows 8.1 update for April 2014 (32-bit, 64-bit)</li><li>• Windows 8.1 update for August 2014 (32-bit, 64-bit)</li><li>• Windows Embedded 8.1 Pro, Industry Pro, and Industry Enterprise (32-bit and 64-bit)</li><li>• Windows 10 (version 1507) (32-bit, 64-bit), including Windows 10 Enterprise 2015 LTSC</li><li>• Windows 10 November Update (version 1511) (32-bit, 64-bit)</li><li>• Windows 10 Anniversary Update (version 1607) (32-bit, 64-bit), including Windows 10 Enterprise 2016 LTSC</li><li>• Windows 10 Creators Update (version 1703) (32-bit, 64-bit)</li><li>• Windows 10 Fall Creators Update (version 1709) (32-bit, 64-bit)</li><li>• Windows 10 April 2018 Update (version 1803) (32-bit, 64-bit)</li><li>• Windows 10 October 2018 Update (version 1809) (32-bit, 64-bit), including Windows 10 Enterprise 2019 LTSC.</li><li>• Windows 10 May 2019 Update (version 1903) (32-bit, 64-bit)</li><li>• Windows 10 November 2019 Update (version 1909) (32-bit, 64-bit) (14.2 RU1 and later)</li><li>• Windows 10 20H1 (Windows 10 version 2004) (14.3 and later)</li><li>• Windows 10 20H2 (Windows 10 version 2009) (14.3 and later)</li><li>• Windows 10 21H1 (as of 14.3 RU1)</li><li>• Windows 11</li></ul>
Operating system (server)	<ul style="list-style-type: none"><li>• Windows Server 2008 R2</li><li>• Windows Small Business Server 2011</li><li>• Windows Server 2012</li><li>• Windows Server 2012 R2</li><li>• Windows Server 2012 R2 update for April 2014</li><li>• Windows Server 2012 R2 update for August 2014</li><li>• Windows Server 2016</li><li>• Windows Server 2019</li><li>• Windows Server, version 1803 (Server Core) (14.2 and later)</li><li>• Windows Server, version 1809 (Server Core)</li><li>• Windows Server, version 1903 (Server Core) (14.2 RU1 and later)</li><li>• Windows Server, version 1909 (Server Core) (14.2 RU1 and later)</li><li>• Windows Server, version 2004</li><li>• Windows Server, version 20H2 (14.3 RU1)</li><li>• Windows Server 2022</li></ul> <p>For a list of supported operating systems for previous releases, see: <a href="#">Windows compatibility with the Endpoint Protection client</a> <a href="#">Endpoint Protection support for Windows 10 updates and Windows Server 2016 / Server 2019</a></p>
Browser Intrusion Prevention	<p>Browser Intrusion Prevention support is based on the version of the Client Intrusion Detection System (CIDS) engine.</p> <p>See <a href="#">Supported browsers for Browser Intrusion Prevention in Endpoint Protection</a></p>

**Table 4: Symantec Endpoint Protection client for Windows hardware system requirements**

Component	Requirements
Processor (for physical computers)	<ul style="list-style-type: none"><li>32-bit processor: 2 GHz Intel Pentium 4 or equivalent minimum (Intel Pentium 4 or equivalent recommended)</li><li>64-bit processor: 2 GHz Pentium 4 with x86-64 support or equivalent minimum</li></ul> <b>Note:</b> Itanium processors are not supported.
Processor (for virtual computers)	One virtual socket and one core per socket at 1 GHz minimum (one virtual socket and two cores per socket at 2 GHz recommended) <b>Note:</b> The hypervisor resource reservation must be enabled.
Physical RAM	1 GB (2 GB recommended) or higher if required by the operating system
Display	800 x 600 or larger
Hard drive	Disk space requirements depend on the type of client you install, which drive you install to, and where the program data file resides. The program data folder is usually on the system drive in the default location C:\ProgramData. Available disk space is always required on the system drive, regardless of which installation drive you choose. <b>Note:</b> Space requirements are based on NTFS file systems. Additional space is also required for content updates and logs.

**Table 5: Symantec Endpoint Protection client for Windows available hard drive system requirements when installed to the system drive**

Client type	Requirements
Standard	With the program data folder located on the system drive: <ul style="list-style-type: none"><li>395 MB*</li></ul> With the program data folder located on an alternate drive: <ul style="list-style-type: none"><li>System drive: 180 MB</li><li>Alternate installation drive: 350 MB</li></ul>
Embedded / VDI	With the program data folder located on the system drive: <ul style="list-style-type: none"><li>245 MB*</li></ul> With the program data folder located on an alternate drive: <ul style="list-style-type: none"><li>System drive: 180 MB</li><li>Alternate installation drive: 200 MB</li></ul>
Dark network	With the program data folder located on the system drive: <ul style="list-style-type: none"><li>545 MB*</li></ul> With the program data folder located on an alternate drive: <ul style="list-style-type: none"><li>System drive: 180 MB</li><li>Alternate installation drive: 500 MB</li></ul>

\* An additional 135 MB is required during installation.

**Table 6: Symantec Endpoint Protection client for Windows available hard drive system requirements when installed to an alternate drive**

Client type	Requirements
Standard	<p>With the program data folder located on the system drive:</p> <ul style="list-style-type: none"> <li>• System drive: 380 MB</li> <li>• Alternate installation drive: 15 MB*</li> </ul> <p>With the program data folder located on an alternate drive:**</p> <ul style="list-style-type: none"> <li>• System drive: 30 MB</li> <li>• Program data drive: 350 MB</li> <li>• Alternate installation drive: 150 MB</li> </ul>
Embedded / VDI	<p>With the program data folder located on the system drive:</p> <ul style="list-style-type: none"> <li>• System drive: 230 MB</li> <li>• Alternate installation drive: 15 MB*</li> </ul> <p>With the program data folder located on an alternate drive:**</p> <ul style="list-style-type: none"> <li>• System drive: 30 MB</li> <li>• Program data drive: 200 MB</li> <li>• Alternate installation drive: 150 MB</li> </ul>
Dark network	<p>With the program data folder located on the system drive:</p> <ul style="list-style-type: none"> <li>• System drive: 530 MB</li> <li>• Alternate installation drive: 15 MB*</li> </ul> <p>With the program data folder located on an alternate drive:**</p> <ul style="list-style-type: none"> <li>• System drive: 30 MB</li> <li>• Program data drive: 500 MB</li> <li>• Alternate installation drive: 150 MB</li> </ul>

\* An additional 135 MB is required during installation.

\*\* If the program data folder is the same as the alternate installation drive, add 15 MB to the program data drive for your total. However, the installer still needs the full 150 MB to be available on the alternate installation drive during installation.

**Table 7: Symantec Endpoint Protection client for Windows Embedded system requirements**

Component	Requirements
Processor	1 GHz Intel Pentium
Physical RAM	<p>256 MB</p> <p><b>Note:</b> This figure is for an installation of the Symantec Endpoint Protection embedded client. If you also implement additional features from an integrated solution such as EDR, additional physical RAM is needed.</p>
Hard drive	<p>The Symantec Endpoint Protection Embedded / VDI client requires the following available hard disk space:</p> <ul style="list-style-type: none"> <li>• Installed to the system drive: 245 MB</li> <li>• Installed to an alternate drive: 230 MB on system drive, and 15 MB on the alternate drive</li> </ul> <p>An additional 135 MB is needed during installation.</p> <p>These figures assume that the program data folder is on the system drive. For more detailed information, or for the requirements of the other client types, see the Symantec Endpoint Protection client for Windows system requirements.</p>

Component	Requirements
Embedded operating system	<ul style="list-style-type: none"> <li>Windows Embedded Standard 7 (32-bit and 64-bit)</li> <li>Windows Embedded POSReady 7 (32-bit and 64-bit)</li> <li>Windows Embedded Enterprise 7 (32-bit and 64-bit)</li> <li>Windows Embedded 8 Standard (32-bit and 64-bit)</li> <li>Windows Embedded 8.1 Industry Pro (32-bit and 64-bit)</li> <li>Windows Embedded 8.1 Industry Enterprise (32-bit and 64-bit)</li> <li>Windows Embedded 8.1 Pro (32-bit and 64-bit)</li> <li>Windows Embedded 10</li> <li>Windows Embedded 11</li> </ul>
Required minimum components	<ul style="list-style-type: none"> <li>Filter Manager (FltMgr.sys)</li> <li>Performance Data Helper (pdh.dll)</li> <li>Windows Installer Service</li> </ul>
Templates	<ul style="list-style-type: none"> <li>Application Compatibility (Default)</li> <li>Digital Signage</li> <li>Industrial Automation</li> <li>IE, Media Player, RDP</li> <li>Set Top Box</li> <li>Thin Client</li> </ul> <p>The Minimum Configuration template is not supported.</p> <p>The Enhanced Write Filter (EWF) and the Unified Write Filter (UWF) are not supported. The recommended write filter is the File Based Write Filter (FBWF) installed along with the Registry Filter.</p>

**Table 8: Symantec Endpoint Protection client for Mac system requirements**

Component	Requirements
Processor/Chip	64-Bit Intel Core 2 Duo or later Apple M1 chip (as of 14.3 RU2)
Physical RAM	2 GB of RAM
Hard drive	1 GB of available hard disk space for the installation
Display	800 x 600
Operating system	<ul style="list-style-type: none"> <li>macOS 10.15 to 10.15.7</li> <li>macOS 11 (Big Sur)</li> </ul> <p>For a list of supported operating systems for previous releases, see: <a href="#">Mac compatibility with the Endpoint Protection client</a></p>

**Table 9: Symantec Endpoint Protection client for Linux system requirements**

Component	Requirements
Hardware	<ul style="list-style-type: none"> <li>Intel Pentium 4 (2 GHz) or later processor</li> <li>1 GB of free RAM (4 GB of RAM is recommended)</li> <li>2 GB available disk space if <code>/var</code>, <code>/opt</code>, and <code>/tmp</code> share the same filesystem or volume</li> <li>500 MB available disk space in each <code>/var</code>, <code>/opt</code>, and <code>/tmp</code> if on different volumes</li> </ul>
Operating systems	<p>Supported operating systems as of version 14.3 RU1:</p> <ul style="list-style-type: none"> <li>Amazon Linux 2</li> <li>CentOS 6, 7, 8</li> <li>Debian 9, 10 (14.3 RU2 and later)</li> <li>Oracle Enterprise Linux 6, 7, 8</li> <li>Red Hat Enterprise Linux 6, 7, 8</li> <li>SuSE Linux Enterprise Server 12.x, 15.x</li> <li>Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS</li> </ul> <p><a href="#">Supported kernels of Symantec Linux Agent</a> (also lists supported minor Linux OS versions)</p> <p>Supported operating systems for version 14.3 MP1 and earlier:</p> <ul style="list-style-type: none"> <li>Amazon Linux</li> <li>CentOS 6U3 - 6U9, 7 - 7U7, 8; 32-bit and 64-bit</li> <li>Debian 6.0.5 Squeeze, Debian 8 Jessie; 32-bit and 64-bit</li> <li>Fedora 16, 17; 32-bit and 64-bit</li> <li>Oracle Linux (OEL) 6U2, 6U4, 6U5, 6U8; 7, 7U1, 7U2, 7U3, 7U4</li> <li>Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9, 7 - 7U8, 8-8U2</li> <li>SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP4, 32-bit and 64-bit; 12, 12 SP1 - 12 SP3, 64-bit</li> <li>SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4, 32-bit and 64-bit; 12 SP3, 64-bit</li> <li>Ubuntu 12.04, 14.04, 16.04, 18.04 (as of 14.3); 32-bit and 64-bit</li> </ul> <p>For a list of supported operating system kernels for previous releases, see <a href="#">List of Linux Distributions and Kernels with Precompiled Auto-Protect Drivers/Modules for Symantec Endpoint Protection for Linux 14.x</a>.</p>
Other environmental requirements (14.3 RU1 and later)	<ul style="list-style-type: none"> <li>OpenSSL 1.0.2k-fips or later</li> </ul>

Component	Requirements
Other environmental requirements (14.3 MP1 and earlier)	<ul style="list-style-type: none"> <li>Glibc Any operating system that runs glibc earlier than 2.6 is not supported.</li> <li>net-tools or iproute2 Symantec Endpoint Protection uses one of these two tools, depending on what is already installed on the computer.</li> <li>Developer tools Auto-compile and the manual compile process for the Auto-Protect kernel module require that you install certain developer tools. These developer tools include gcc and the kernel source and header files. For details on what to install and how to install them for specific Linux versions, see: <a href="#">Manually compile Auto-Protect kernel modules for Endpoint Protection for Linux</a></li> <li>i686-based dependent packages on 64-bit computers Many of the executable files in the Linux client are 32-bit programs. For 64-bit computers, you must install the i686-based dependent packages before you install the Linux client. If you have not already installed the i686-based dependent packages, you can install them by command line. This installation requires superuser privileges, which the following commands demonstrate with <code>sudo</code>: <ul style="list-style-type: none"> <li>For Red Hat-based distributions: <code>sudo yum install glibc.i686 libgcc.i686 libX11.i686 libns1.i686</code></li> <li>For Debian-based distributions: <code>sudo apt-get install ia32-libs</code></li> <li>For Ubuntu-based distributions: <code>sudo dpkg --add-architecture i386</code> <code>sudo apt-get update</code> <code>sudo apt-get install gcc-multilib libx11-6:i386</code></li> </ul> </li> </ul>
Graphical desktop environments	<p>You can use the following graphical desktop environments to view the Symantec Endpoint Protection for Linux client:</p> <ul style="list-style-type: none"> <li>KDE</li> <li>Gnome</li> <li>Unity</li> </ul> <p>Symantec Agent for Linux 14.3 RU1 does not have a graphical user interface.</p>

[Release versions, notes, new fixes, and system requirements for Endpoint Security and all versions of Endpoint Protection](#)

## Known issues and workarounds for Symantec Endpoint Protection (SEP)

The items in this section apply to this release of Symantec Endpoint Protection.

### NOTE

The Issue column displays the version number when the issue appears. For example, [14.3 RU1] means that the issue applies to version 14.3 RU1 and later. When these issues are fixed, they appear in the fix-it notes: [Versions, system requirements, release dates, notes, and fixes for Symantec Endpoint Protection and Endpoint Security](#)

**Table 10: Upgrade issues**

Issue	Description and solution
The following error message appears: "Symantec Endpoint Protection version 14.3 RU2 for Win64bit is the latest package. You cannot delete it." [14.3 RU2]	You cannot delete the Client Install Package when packages from multiple builds appear in the Symantec Endpoint Protection Manager. As of 14.3 RU2, LiveUpdate can download multiple client installation packages with a different build number, which appear in the <b>Admin</b> page > <b>Install Packages</b> > <b>Client Install Package</b> table. [SEP-72531]
AutoUpgrade fails if you use the 14.3 RU2 <b>Upgrade to English if currently installed language is unsupported</b> option to upgrade clients with an unsupported language to English. [14.3 RU2]	<p>This issue occurs for clients that you manually upgraded from a supported to an unsupported language in 14.3 RU1 MP1 and earlier, such as upgrading a Czech client to a Japanese client on a Japanese operating system. And then used to the <b>Upgrade to English if currently installed language is unsupported</b> option to upgrade the unsupported language to English in 14.3 RU2. [SEP-72490]</p> <p>This issue is caused because the client language uses the language of the supported operating system (in this case, Japanese). AutoUpgrade expects to use the supported language and not English.</p> <p>To work around this issue, try the AutoUpgrade again and turn off the <b>Upgrade to English if currently installed language is unsupported</b> option.</p>
When exporting a client installation package from a 14.3 RU2 Symantec Endpoint Protection Manager (SEPM), the following warning message appears: "The client installation package does not have content." [14.3 RU2]	<p>This issue occurs when communication between the Symantec Endpoint Protection Manager and the console being used to export the package is disrupted.</p> <p><a href="#">"The client installation package does not have content." warning when exporting an installation package from the Endpoint Protection Manager</a></p>
An error appears when importing the most recent client installation packages into an older version of Symantec Endpoint Protection Manager. [14.3 RU2]	Symantec Endpoint Protection 14.3 RU2 clients cannot be managed by a 14.3 RU1 MP1 or earlier Symantec Endpoint Protection Manager. [SEP-72292]
After upgrading a Symantec Endpoint Protection Manager to 14.3 RU2, php-cgi.exe crashes with an error in the event viewer [14.3 RU2]	<p>This issue occurs with the 17.4.1.1 version of the Microsoft ODBC Driver for SQL Server. [SEP-70385]</p> <p>To work around this issue, download and install the 17.7.2 version of the Microsoft ODBC Driver for SQL Server on Windows: <a href="https://docs.microsoft.com/en-us/sql/connect/odbc/windows/release-notes-odbc-sql-server-windows?view=sql-server-ver15">https://docs.microsoft.com/en-us/sql/connect/odbc/windows/release-notes-odbc-sql-server-windows?view=sql-server-ver15</a></p> <p><a href="#">php-cgi.exe crash occurs on Endpoint Protection Manager after upgrading to 14.3 RU2</a></p>
After upgrading to Symantec Endpoint Protection Manager 14.3 RU2, "The client computer has been renamed" notifications may appear [14.3 RU2]	<p>After upgrading from an older version of Symantec Endpoint Protection Manager to 14.3 RU2, administrators may start receiving "The client computer has been renamed" notifications. This issue is applicable only to Mac clients.</p> <p><a href="#">"The client computer has been renamed" notifications may appear after upgrading to Symantec Endpoint Protection Manager 14.3 RU2</a></p>
A Symantec Endpoint Protection Manager in a dark network downloads old Client Intrusion Detection System (CIDS) content to new clients because LiveUpdate does not run during an upgrade [14.3 RU1]	<p>When a 14.3 RU1 Symantec Endpoint Protection Manager cannot access either the Internet or a LiveUpdate Administrator (LUA) server, it keeps old, incompatible content in its cache. This old content is normally delivered to the new clients. To update the content in the management server's cache, you manually download certified virus definitions and CIDS .jdb files. [SEP-69125]</p> <p>To make sure that the new clients do not get old content, manually install a CIDS .jdb file on SEPM before you install new clients or upgrade old clients.</p> <p><a href="#">Download .jdb files to update definitions for Endpoint Protection Manager</a></p>

Issue	Description and solution
Cannot log on to Symantec Endpoint Protection Manager (SEPM) when the network interface card is disabled [14.3 RU1]	<p>If after you install Symantec Endpoint Protection Manager, you cannot log on to the console and the following error message appears:</p> <p>Unexpected server error</p> <p>This issue may occur if the computer's network interface card is disabled when you installed the SEPM, which keeps the server certificate from being generated. [SEP-67040]</p> <p>To find out if SEPM was installed with a disabled network interface card, look at the server certificate.</p> <p><a href="#">Unexpected server error at SEPM login if it was installed on a server without an enabled NIC</a></p>
When you uninstall SEPM and use the option to remove the default database and leave the SQL Server Express instance, the following error appears: "An error occurred while trying to connect to the database server" [14.3 RU1]	<p>If you uninstall the Symantec Endpoint Protection Manager and select the <b>Remove only the DB and leave the SQL Server Express instance installed with SEPM</b> option, you may see the following error: "An error occurred while trying to connect to the database server." This issue occurs after you add the credentials for the default user DBA and may be related to user privileges. [SEP-68670]</p> <p>To work around this issue, perform the uninstallation by running the SEPM setup.exe file and clicking the <b>Remove only the DB and leave the SQL Server Express instance installed with SEPM</b> option during uninstallation.</p>
A SQL Server upgrade from version 2017 to version 2019 fails with FIPS mode enabled [14.3]	<p>You may see the error: "The following error has occurred. An error occurred while installing extensibility feature with error message: AppContainer Creation Failed with error message NONE, state. This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms." This occurs if you have a FIPS-enabled Symantec Endpoint Protection Manager 14.3 and you upgrade from the Microsoft SQL Server 2017 to 2019. [SEP-61473]</p> <p>To work around this issue, disable FIPS at the operating system level:</p> <ol style="list-style-type: none"> <li>1. In C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools, click <b>Local Security Policy &gt; Local Policies &gt; Security Options</b>, and disable <b>System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing</b></li> <li>2. Upgrade from SQL Server version 2017 to version 2019.</li> <li>3. After SQL Server upgrades successfully, re-enable FIPS.</li> </ol> <p><a href="#">SQL upgrade from 2017 to 2019 fails with FIPS mode enabled</a></p>
Custom names may prevent the firewall policy from updating during an upgrade to 14.2 or later	<p>For an upgrade to Symantec Endpoint Protection 14.2 or later, firewall policies cannot incorporate the changes for IPv6 if you changed some default names. The default names include the names of default policies and default rule names. If the rules cannot be updated during the upgrade, the IPv6 options do not appear. Any new policies or rules that you create after the upgrade are not affected.</p> <p>If possible, revert any changed names back to the default. Otherwise, ensure that any custom rules that you added to a default policy do not block IPv6 communication in any way. Ensure the same for any new policies or rules that you add.</p>



**Table 11: Symantec Endpoint Protection Manager issues**

Issue	Description and solution
Some EDR events do not appear on the client [14.3 RU1]	The Symantec Endpoint Protection client must run Windows 10 build 14393 or later to collect Symantec EDR Event Tracing for Windows (ETW) events. [SEP-67175]
The Network Traffic Redirection feature has some limitations [14.3 RU1]	<ul style="list-style-type: none"> <li>• The Symantec Web Security Service is delivered on IPv4 and not IPv6. [SEP-68700]</li> <li>• The tunnel redirection method: <ul style="list-style-type: none"> <li>– Runs on Windows 10 x64 version 1703 and later (Semi-Annual Servicing Channel) only. This method does not support any other Windows operating systems or the Mac client. [SEP-67927]</li> <li>– Does not support HVCI-enabled Windows 10 64-bit devices. [SEP-67648]</li> <li>– Redirects outbound traffic from the Symantec Endpoint Protection client to the WSS before it gets evaluated by either the client's firewall or the URL reputation rules. Instead, that traffic is evaluated against the WSS firewall and the URL rules. For example, if a SEP client firewall rule blocks google.com and a WSS rule allows google.com, the client allows users to access google.com. Inbound local traffic to the client is still processed by the Symantec Endpoint Protection firewall. [SEP-67488]</li> <li>– The WSS Captive Portal is not available for the tunnel method, and the client ignores the challenge credentials. In a future release, SAML authentication in the WSS agent will replace the Captive Portal, and will be available in the Symantec Endpoint Protection client.</li> <li>– If a client computer connects to the WSS using the tunnel method and hosts virtual machines, each guest user needs to install the SSL certificate provided in the WSS portal.</li> <li>– Traffic for local network like your home directory or Active Directory authentication is not redirected.</li> <li>– Is not compatible with the Microsoft DirectAccess VPN.</li> </ul> </li> </ul> <p>The tunnel method is currently considered an early adopter release feature.</p>
Duplicate client enrollment entries after the upgrade from 14.2.x to 14.3 MP1 and later [14.3 RU1]	<p>Upgrading the Symantec Endpoint Protection clients from 14.2.x to 14.3 MP1 and later creates duplicate agent enrollment entries for these clients on the <b>Clients</b> page in Symantec Endpoint Protection Manager.</p> <p>There is no functional impact and you can continue working with the new entries for 14.3 RU1 clients. Symantec Endpoint Protection Manager will remove older agent entries.</p>
Allow URLs in Symantec Endpoint Security if you use the hybrid management option, proxy servers or a perimeter firewall [14.3]	<p>With Broadcom's acquisition of Symantec Enterprise Security, the URLs for client-to-cloud communication changed in 14.2.2.1. [CDM-42467]</p> <p>You must upgrade your clients to version build 14.2.5569.2100 or later in the following situation</p> <ul style="list-style-type: none"> <li>• You use Symantec Endpoint Security to manage your clients and policies when your on-premises Symantec Endpoint Protection Manager domains are enrolled in the cloud console</li> <li>• You use proxy servers.</li> </ul> <p>You allow the URLs in either fully cloud-managed or hybrid-managed agents, allow their your proxy server and/or perimeter firewall.</p> <p>See <a href="#">URLs that allow SEP and SES to connect to Symantec servers</a></p> <p>See <a href="#">Upgrade cloud-managed Symantec Agents to version 14.2 RU2 MP1 or later.</a></p>
The Symantec Endpoint Protection Manager remote console no longer supports the 32-bit Windows platform [14.3]	<p>In 14.3 and later, you cannot log on to the Symantec Endpoint Protection Manager remote console if you run a 32-bit version of Windows. The Oracle Java SE Runtime Environment no longer supports 32-bit versions of Microsoft Windows. [SEP-61106]</p> <p>If you see the following message, log on to Symantec Endpoint Protection Manager locally:</p> <p>"This version of C:\Users\Administrator\Downloads\Symantec Endpoint Protection Manager Console\bin\javaw.exe is not compatible with the version of Windows you're running. Check your computer's system information and then contact the software publisher."</p>

Issue	Description and solution
"Failed to install Microsoft Visual C++ Runtime" error appears while you install Symantec Endpoint Protection Manager [14.3]	You may see the following error while installing the Symantec Endpoint Protection Manager on Windows 2012 R2: "Failed to install Microsoft Visual C++ Runtime" [SEP-60396] To work around this issue, activate Windows and install the Windows updates. The Windows update installs the Visual C++ 2017 redistributable, which is a prerequisite for the Symantec Endpoint Protection Manager 14.3 installation on Windows 2012 R2.
Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows [14.3]	After you upgrade to or install a Symantec Endpoint Protection Manager version 14.3 that is enrolled in the cloud console, the management server no longer uploads logs successfully to the cloud. In the uploader.log you may see the following error: <code>&lt;SEVERE&gt; WinHttpSendRequest: 12175: A security error occurred</code> This issue is caused by a missing Microsoft update that provides support for TLS 1.1 and 1.2. To solve the issue, install Microsoft update: KB3140245. For more information, see: <a href="#">Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows</a>
"Deployment in progress" still appears in Symantec Endpoint Protection Manager after the client receives an updated policy for Endpoint Threat Defense for AD [14.2 RU1 MP1 and later]	This behavior is expected. Endpoint Threat Defense for AD 3.3 policies are only supported on the client as of version 14.2 RU1 MP1. You apply a policy for Symantec Endpoint Threat Defense for Active Directory 3.3 to a group. This group contains some clients that run Symantec Endpoint Protection 14.2 RU1 or earlier. These clients receive and apply the policy as expected, but the status in Symantec Endpoint Protection Manager continues to show the message Deployment in progress.

**Table 12: Windows, Mac, and Linux client issues**

Issue	Description and solution
You must restart the rebootless Windows client to obtain latest EDR events [14.3 RU3]	To make additional ETW events available in 14.3 RU3, you must restart the Symantec Endpoint Protection client. You must restart the client in the following situations: [SEP-73327] <ul style="list-style-type: none"> <li>If EDR is enabled and you update the client to RU3.</li> <li>14.3 RU3 is already installed and you enable or disable EDR. You must restart the client to enable or disable the newly added events.</li> </ul>
Scan Engine fails to initialize after the Linux client upgrade. [14.3 RU3]	Scan Engine fails to initialize after upgrading Symantec Endpoint Protection client for Linux to version 14.3 RU3. <b>Workaround:</b> <ol style="list-style-type: none"> <li>Update the LiveUpdate Server with latest content that would have SEF 1.7.6.</li> <li>Uninstall Linux client 14.3 RU3 that is exhibiting the "Scan Engine initialization failure" error.</li> <li>Reinstall Linux client 14.3 RU3.</li> </ol>
auditd daemon will be enabled after the Linux client installation. [14.3 RU3]	Symantec Endpoint Protection client for Linux installer enables auditd daemon after the agent installation even if auditd daemon was disabled before the installation.
Possible connection issues on Mac devices. [14.3 RU2]	<ul style="list-style-type: none"> <li>After upgrading the Mac agent using AutoUpgrade and restarting the device, the agent might fail to connect to the network. <b>Workaround:</b> Rerun the agent installation package.</li> <li>After being in standby mode, a Mac device might lose its network connection with the following error: "Your connection was interrupted. A network change was detected." <b>Workarounds:</b> <ul style="list-style-type: none"> <li>If you use a docking station, renew the IP addresses manually at <b>System Preferences &gt; Network</b>.</li> <li>Unplug the docking station from your Mac device for a few seconds and then plug it in again.</li> </ul> </li> </ul>

Issue	Description and solution
Rosetta may block the Mac agent installation on Apple Silicon (M1) devices with the following error: "This version of Symantec Agent for Mac is not supported on Apple M1 chip." [14.3 RU2]	For more information, see <a href="#">KB 222282</a> .
Downloading and installing Mac agent using the Web link that was generated in Symantec Endpoint Protection Manager may fail. [14.3 RU2]	<p>If an admin invites users to install the Mac agent 14.3 RU2 using the <b>Web Link and Email</b> option in Symantec Endpoint Protection Manager and the users download the package using this link in the Safari browser, the installation of the Mac agent may fail with the following error:</p> <p>"The application Symantec Endpoint Protection Installer can't be opened"</p> <p><b>Workarounds:</b></p> <ul style="list-style-type: none"> <li>After downloading the file, go to the <b>Downloads</b> folder, execute the following command, and then run the installation again:  <code>chmod +x ./Symantec\ Endpoint\ Protection\Symantec\ Endpoint\ Protection\ Installer.app/Contents/MacOS/Symantec\ Endpoint\ Protection\ Installer</code></li> <li>Open Safari browser's <b>Preferences</b> and on the <b>General</b> tab, uncheck the option <b>Open "safe" files after downloading</b>. Then download the installer package, and run the installation.</li> </ul>
If you automatically upgrade a client with an unsupported language to English, the client continues to display the date settings for definitions in English [14.3 RU1 and later]	To work around this issue, uninstall the legacy client and manually install a new English client installation package. In addition, a fix is expected for clients that are upgraded automatically. [SEP-72481]
The standalone Symantec WSS Agent blocks the Symantec Endpoint Protection client installation if you install SEP on the same computer as the WSS Agent	<p>The Network Traffic Redirection (NTR) component uses the same files as the standalone Symantec WSS Agent (WSSA). NTR is installed by default in both Symantec Endpoint Protection and the Symantec Endpoint Security cloud console. If the NTR feature is installed on an endpoint, WSSA can not be installed. Similarly, if WSSA is installed, the NTR feature does not install.</p> <p>You can remove the Network Traffic Redirection feature from existing endpoints without having to uninstall the whole client by using one of the following methods:</p> <ul style="list-style-type: none"> <li>In Symantec Endpoint Protection Manager, create a Client Install Feature Set that does not include NTR and apply it to the endpoints.  <a href="#">Add or remove features to existing Endpoint Protection clients</a></li> <li>The following command line option uses the client installation file to remove NTR:  <code>setup.exe /s /v" REMOVE=NTR /qn"</code></li> </ul>
Upgrade installation package that is used for clean installation installs default feature set. [14.3 RU1 MP1 and earlier]	<p>If you create an upgrade installation package with <b>Maintain existing client features when updating</b> option checked, and use this package to do a clean installation, the default feature set will be installed on your client device.</p> <p>If you want to install a custom feature set, you must create a separate installation package for the clean installation.</p>
Unsupported upgrade path creates duplicate devices in cloud console. [14.3 RU1]	<p>Upgrading your macOS from 10.15 to 11.0 before upgrading the Symantec Agent for Mac from 14.2/14.3 to 14.3 RU1 creates duplicate devices in cloud console.</p> <p>To avoid duplicates, you must upgrade the client before upgrading the operating system (i.e. upgrade the Symantec Agent for Mac from 14.2/14.3 to 14.3 RU1 and then upgrade macOS from 10.15 to 11.0.).</p>
Incorrect messages in the Symantec Agent for Linux installer log. [14.3 RU1]	<p>In some cases, the agent installer logs incorrect messages related to a non-matching driver version or a required reboot.</p> <p>These messages do not affect the functionality of the agent.</p>

Issue	Description and solution
On a SuSe Linux device, zypper removes the SEP Linux client packages while removing the 'at' package. [14.3 RU1]	On a SuSe Linux device, the command 'zypper remove at' removes the SEP Linux client packages because the 'at' package is added as a required dependent package and the zypper commands automatically attempt to remove the SEP client packages 'sdcss-kmod' and 'sdcss-sepagent' as the packages with unused dependencies. <b>Workaround:</b> To remove the 'at' package, run the following command: rpm -e --nodeps at
Upgrade issue on macOS 10.15 and later [14.3 MP1]	On macOS 10.15 and later, the <b>Install Symantec Endpoint Protection to Remote Computers</b> feature in the Client Deployment Wizard fails to upgrade the Symantec Endpoint Protection client from older versions to version 14.3 MP1. <b>Workaround:</b> Use <b>Symantec Endpoint Protection Manager Auto Upgrade</b> to perform the Symantec Endpoint Protection client upgrade on macOS 10.15 and later.
The Symantec Endpoint Protection 14.3 Windows client installation may fail unless you first install SHA-2 support [14.3]	If you run legacy operating system versions (Windows 7 RTM or SP1, Windows Server 2008 R2 or R2 SP1 or R2 SP2), you are required to have SHA-2 code signing support installed on your devices to install Windows updates released on or after July 2019. Without SHA-2 support, the Windows client installation sometimes fails. The installation may fail whether you install clients for the first time or automatically upgrade from a previous release. [SEP-61175/61403] To get Microsoft enforced SHA-2 code signing support, see: <a href="#">2019 SHA-2 Code Signing Support requirement for Windows and WSUS</a> <a href="#">Symantec Endpoint Protection 14.3 Windows client may fail to install unless SHA-2 support is installed</a>
The Symantec Endpoint Protection Windows client does not run when installed on Windows 10 1803 with UWF enabled [14.3]	If the Symantec Endpoint Protection client runs on the Windows 10 RS4 1803 32-bit operating system when the Unified Write Filter (UWF) is enabled and protecting the drive on which the Windows client is installed, the client does not run properly. This Windows operating system contains a UWF defect that prevents the Windows client from running. To work around this issue: <ul style="list-style-type: none"> <li>• Upgrade to another operating system version that does not contain the defect.</li> <li>• Disable UWF. See: <a href="#">Endpoint Protection is malfunctioning when installed on Windows 10 1803 with UWF enabled</a></li> </ul>
Mac clients that enable WSS Traffic Redirection do not honor custom proxy settings for LiveUpdate [14.2 RU1 MP1 and later]	You have configured your managed Mac clients for Symantec Endpoint Protection 14.2 RU1 MP1 or later to use custom proxy settings for LiveUpdate through External Communications Settings. After you enable WSS Traffic Redirection (WTR) for your Mac clients through the Symantec Endpoint Protection Manager policy, however, you find that LiveUpdate traffic no longer honors your custom proxy settings. Instead, LiveUpdate attempts a direct connection. To work around this issue, only use custom proxy settings for LiveUpdate when WSS Traffic Redirection is disabled.
Microsoft Edge unexpectedly allows PDF downloads with Hardening enabled [14.2 RU1 MP1 and later]	With Application Hardening enabled in the Symantec Endpoint Protection client, you are unexpectedly able to download PDF files if you use the Microsoft Edge browser. The prevention of the download of PDF files works as expected with other browsers. A fix for this issue is planned for a future release.

With Broadcom's recent announcement that Symantec Enterprise Protection has officially joined Broadcom, Symantec migrated the documentation to the Broadcom [Symantec Security Tech Docs Portal](#).

To find Endpoint Protection documentation, click the **Symantec Security Software** tab, then click **Endpoint Security and Management > Endpoint Protection**.

---

**Table 13: Documentation issues**

Issue	Description and solution
HOWTO articles have been expired.	The HOWTO articles, which were duplicates of the topics in the Symantec Endpoint Protection Manager Help, have been republished on the <a href="#">Endpoint Protection</a> site and now have a different URL. To find an article, use the <b>Search field</b> .
PDF files	Symantec posted all PDF files on DOC articles. These pages have been expired. To find the release most recent version of the PDF file, go to the <a href="#">Related Documents</a> page. In the future, Broadcom will be adding legacy PDF files and translated PDF files.

For resolved issues, see:

[New fixes and components for Symantec Endpoint Protection 14.3 RU1 MP1](#)

[New fixes and components for Symantec Endpoint Protection 14.3 RU1](#)

[New fixes and components for Symantec Endpoint Protection 14.3 MP1](#)

[New fixes and components for Symantec Endpoint Protection 14.3](#)

## Supported virtual installations and virtualization products

You can install Symantec Endpoint Protection on the supported operating systems that run in virtual environments. Install Symantec Endpoint Protection on the guest operating system, and not the host.

The following virtualization products support the Symantec Endpoint Protection Manager, console, and Symantec Endpoint Protection client software for Windows and Linux:

- 
- Microsoft Azure
  - Amazon WorkSpaces
  - Citrix Studio Version 2009.0.0
  - Nutanix AOS 5.15 (LTS)
  - VMware WS 5.0 (workstation) or later
  - VMware GSX 3.2 (enterprise) or later
  - VMware ESX 2.5 (workstation) or later
  - VMware ESXi 4.1 - 5.5
  - VMware ESXi 6.0
  - VMware ESXi 6.0 Update 1
  - VMware ESXi 6.0 Update 2
  - VMware ESXi 6.0 Update 3 (As of 14.0.1)
  - VMware ESXi 6.5 (As of 14.0.1)
  - VMware ESXi 6.5U1 (As of 14.2)
  - VMware ESXi 6.5U2 (As of 14.2)
  - VMware ESXi 6.7 (As of 14.2)
  - VMware ESXi 7.0 Update 2 (As of 14.3 RU2)
  - Microsoft Virtual Server 2005
  - Windows Server 2008 Hyper-V
  - Windows Server 2012 Hyper-V
  - Windows Server 2012 R2 Hyper-V
  - Windows Server 2016 Hyper-V (As of 14.2 MP1)
  - Windows Server 2019 Hyper-V Core Edition (As of 14.2 MP1)
  - Citrix XenServer 5.6 or later
  - Virtual Box, supplied by Oracle

Symantec Endpoint Protection includes many features that enhance performance in virtual environments.

[Using Symantec Endpoint Protection Manager in virtual infrastructures](#)

[Randomizing scans to improve computer performance in virtualized environments on Windows clients](#)

For the most current system requirements, see: [Release Notes and System Requirements for all versions of Symantec Endpoint Protection](#)

## About Endpoint Protection release types and versions

In the Symantec Endpoint Protection (SEP) product interface or documentation, you may see references to a Release Update or a Maintenance Patch. For release versions, you may see a number with three decimal points, such as 14.0.1.0. You want more information about what these terms mean, how they relate to the release version number, and how Symantec Endpoint Protection versioning works.

### Release terminology definitions

- **Major Release**

A Major Release is a new software product release that incorporates all updates since the last Major Release. A Major release also provides additional enhancements to the software, such as architectural changes, major feature changes, or new platform or operating system support. A Major Release typically requires a new installation, but does not always.

Reading from left to right, the numbers to the left of the first decimal point typically signify the Major Release version.

- **Minor Release**

---

A Minor Release updates the previous Major Release. The update incorporates all previous updates since the last Major Release. A Minor Release is tied to the Major Release, and may also contain new features, or new platform or operating system support.

Reading from left to right, the numbers between the first and second decimal point typically signify the Minor Release version.

- **Release Update**

A Release Update provides low-risk new features or support for additional platforms, in addition to fixes, following the release of Major or Minor Releases.

Reading from left to right, the numbers between the second and third decimal point typically signify the Release Update version.

- **Maintenance Patch**

A Maintenance Patch delivers adaptive, corrective, and perfective low-risk maintenance for Major or Minor Releases. A Maintenance Patch is sometimes also called a Maintenance Pack.

Reading from left to right, the numbers to the right of the third decimal point typically signify the Maintenance Patch version.

For example, for the release version 14.3.2.1:

- 14 represents the Major Release version.
- 3 represents the Minor Release version.
- 2 represents the Release Update version.
- 1 represents the Maintenance Patch version.

Occasionally, you may see release versions that are expressed using the abbreviations RU (for Release Update) or MP (for Maintenance Patch). For example, you may instead see references to 14.3 RU2 MP1, or more commonly to 14.3.2 MP1. Both are equivalent to 14.3.2.1.

#### **NOTE**

The product release version may be different from the product build version that is found in the product user interface. For a list of build versions as they compare to release versions, see:

[Released versions of Symantec Endpoint Protection](#)

### **How Symantec releases updates for Symantec Endpoint Protection**

Symantec releases cumulative updates for Symantec Endpoint Protection. A new Release Update contains new updates and updates from Maintenance Patches that were created for the previous Release Update. Maintenance Patches are created only for the most recent Release Update.

For example, 14.0.1 (14 RU1) includes new updates as well as updates from 14 MP1 and 14 MP2. After the release of 14.0.1, no further Maintenance Patches are created or released for version 14. Instead, they branch off of 14.0.1.

[Installing Endpoint Protection client patches on Windows clients](#)

## **Where to get more information**

The following table displays the websites where you can get best practices, troubleshooting information, and other resources to help you use the product.



**Table 14: Endpoint Protection website information**

Types of information	Website link
Trial versions	Contact your account representative.
Manuals and documentation updates	<a href="#">Related Documents</a> page For other languages, click the <b>English</b> drop-down menu.
Technical Support	<a href="#">Endpoint Protection Technical Support</a> Includes knowledge base articles, product release details, updates and patches, and contact options for support.
Threat information and updates	<a href="#">Symantec Security Center</a>
Training	<a href="#">Education Services</a> Access the training courses, the eLibrary, and more.
Symantec Connect forums	<a href="#">Endpoint Protection</a>

## What's new for all releases of Symantec Endpoint Protection (SEP) 14.x

You can view a list of the changes for all versions of Symantec Endpoint Protection 14. This list includes the added operating system support, added browser support, and the new feature changes.

The changes for the Windows clients also apply to those managed by the Integrated Cyber Defense Manager (ICDm) cloud console. The cloud-managed clients (also called Symantec Agents) are the same as the on-premises managed clients.

- You can manage client version (14.2 RU1) 14.2.3332.1000 or later with Symantec Endpoint Protection Manager 14.2 RU1 or later, or fully in the cloud.
- You can manage fully in the cloud as of client version (14.2 RU1 (cloud-managed only)) 14.2.2486.1000.
- You can manage client version (14.0.1 / 14.1) 14.0.3752.1000 with Symantec Endpoint Protection Manager 14 RU1 or later, or partially in the cloud.

[Release notes, new fixes, and system requirements for Endpoint Security and all versions of Endpoint Protection](#)  
(includes release numbers, release dates, build numbers)

[Product guides for all versions of Symantec Endpoint Protection 14](#)

### Version 14.3 RU2

- Includes runtime protection against fileless threats such as malicious Excel macros (XLM) and payloads using Windows Management Instrumentation (WMI) with our expanded integration with Antimalware Scan Interface (AMSI).
- Enhanced behavior detection and prevention protects against ransomware families such as Ryuk and Netwalker with improved behavioral detection and prevention of malicious modification or removal of user files.
- A **browser extension** provides better protection for both HTTP and HTTPS traffic to and from the Google Chrome web browser. The client blocks users from accessing malicious sites and redirects users to a default landing page. The browser extension depends on IPS; therefore, the IPS policy must be enabled and assigned to the group. The browser extension is downloaded from LiveUpdate by default if the computer joined an Active Directory domain. Otherwise, the browser extension is downloaded from the Google Web Store.
- Ability for administrators to retrieve quarantined files on remote clients from the Symantec Endpoint Protection Manager console. These malicious files can be used for further investigating and sandboxing. To upload the quarantined file, the new **Upload quarantined files from the clients** option automatically uploads all quarantined files from the clients. You can then select and retrieve individual files from the Risk log using the **Download file that the**



---

**client quarantined** command. The management server no longer supports old versions of the Central Quarantine Server.

- Intrusion Prevention (IPS) content has been optimized considerably to reduce content size and improve network throughput. This improvement is available to all supported Symantec Endpoint Protection versions.
- Includes automatic LiveUpdate for critical fixes and security updates. Starting with SEP 14.3 RU2, critical patches and security fixes are delivered automatically to clients via LiveUpdate to reduce the administrative burden of managing agent updates. These patches include critical fixes only; new features are delivered separately via Release Updates (RUs).
- Both the Symantec Endpoint Protection clients and the Symantec Endpoint Protection Manager is localized in the following five languages only: English, French, Spanish, Portuguese, and Japanese. You can automatically upgrade the client language to English if the previous clients' language is unavailable using the **Upgrade to English if unsupported language is unavailable** option. If you do not choose English, the clients with an unsupported language do not get upgraded.
- Location awareness has four new criteria: the computer's host name, user and group name, operating system, and whether a particular file runs on the client.

#### [What's new for Symantec Endpoint Protection 14.3 RU2?](#)

##### **Version 14.3 RU1 MP1**

- Added ability to log in to Symantec Endpoint Protection Manager using credentials in AD format (i.e. username@domain.com or domain\username).
- The new option **Maintain existing client features when updating** under **Installation Features and Settings** lets you create and export a client package that will only upgrade the client to a new version but will make no changes to the configuration, client communication, or installed features.
- Antimalware AMSI Scan now takes the file/folder exceptions into account when scanning a script file before it runs.

#### [What's new for Symantec Endpoint Protection 14.3 RU1 MP1](#)

##### **Version 14.3 RU1**

- Includes the new Symantec Mac Agent and the Symantec Linux Agent that can be installed and managed from either the on-premises Symantec Endpoint Protection Manager or the Integrated Cyber Defense Manager cloud console.
- Prevents new and unknown threats on the macOS using behavioral protection, or SONAR.
- Blocks untrusted non-portable executable (PE) files such as PDF files and scripts that are not yet identified as a threat with a File Access Exception.
- Prevents web threats based on the reputation score of a web page. The Intrusion Prevention policy includes URL reputation filtering, which blocks web pages with reputation scores below a specific threshold.
- The embedded database was updated to the Microsoft SQL Express database. The SQL Server Express database stores policies and security events more efficiently than the default embedded database and is installed automatically with the Symantec Endpoint Protection Manager.

#### [What's new in Symantec Endpoint Protection 14.3 RU1](#)

##### **Version 14.3 MP1 (refresh)**

Added support with Google Cloud Platform for cloud-enrolled Symantec Endpoint Protection Managers and cloud-managed Symantec Agents. You do not need to upgrade if you continue to use the on-premises Symantec Endpoint Protection Manager to entirely manage your clients. See: [FAQ: Migration of Symantec Endpoint Protection to Google Cloud Platform](#)

##### **Version 14.3 MP1**

- 
- A REST API enhancement lets you copy over settings in the **General Settings** policy to other groups.
  - External Logging adds a new Syslog entry containing PII filtered policy changes. This change adds a second log line containing the policy payload when a policy change is made and recorded in the Audit log.
  - External Logging forwards information about the type of scan to Syslog servers. This information includes whether the scan was a full scan or active scan and a manual or scheduled scan. This change adds a new SCAN\_TYPE column in External Logging for scan events. You can use this information to track regularly scheduled scans on your client computers.
  - The Symantec Endpoint Protection Manager Administrative Log displays the administrator's user name and the source and destination group names after a client moves from one group to another.
  - Added command-line scan support for the Windows Subsystem for Linux (WSL) processes. Dependent on SDS 1.12 or later.
  - The database schema includes table changes in SEM\_AGENT and SERVER\_POLICY\_LOG\_1 and 2.

#### [What's new for Symantec Endpoint Protection 14.3 MP1](#)

##### **Version 14.3**

- Integration with Antimalware Scan Interface (AMSI).
- Enhanced support for web applications with WSS PAC file redirection allows administrators to customize the proxy auto configuration file hosted by WSS Local Proxy Service.
- Symantec Endpoint Protection Manager and remote console now supports Java 11.
- External logging failover.
- Support for Windows 10 version 2004 and SQL Server 2019.
- Linux agents now supports Ubuntu 18.04, RHEL 8, and CentOS 8.

#### [What's new for Symantec Endpoint Protection 14.3](#)

##### **Version 14.2 RU2 MP1 (refresh)**

- URL update for hybrid-managed Symantec Agents with an Application Isolation and Application Control policy. See: [Upgrade cloud-managed Symantec Agents to version 14.2 RU2 MP1](#) for more detail.

##### **Version 14.2 RU2 MP1**

- The Integrations policy includes a new option, Allow direct traffic when WSS protection is not available. You use this option to give users access to the web if user authentication with the WSS cloud proxy (ProxySG) fails. This situation occurs if the administrator sets up WSS Traffic Redirection, but not the WSS roaming users.
- A REST API enhancement lets you query the Location Awareness policy assigned to clients.
- The Syslog logs for Splunk differentiate whether a scan is a full system scan, quick scan, a manual scan, or a scheduled scan. The logs also show a new "Location" column in External Logging for SONAR protection events.
- Support was added for email addresses and distribution lists with special characters for Symantec Endpoint Protection Manager notifications.
- Added the following operating system support for the Linux client: Red Hat Enterprise Linux Server (RHEL) 8 and 8.1, CentOS 8 with Kernel 4.18
- Upgraded Jackson-databind and SQLite third-party components.

##### **Version 14.2 RU2**

- Support for:
  - Windows 10 19H2 (version 1909)
  - macOS 10.15 (Catalina)
- Upgraded multiple third-party components to newer versions.

##### **Version 14.2 RU1 MP1 (refresh)**

*Release date: 24 Sept 19*

---

No new features or enhancements.

#### [New fixes and component versions in Endpoint Protection 14.2 RU1 MP1](#)

##### **Version 14.2 RU1 MP1**

Release date: 4 August 2019

- Made improvements for cloud-managed clients:
  - Added the Vulnerability Remediation plug-in.  
This feature identifies missing critical Windows updates, and lets the administrator apply those updates through Windows Update from the cloud console.  
Support for this feature in the cloud console is slated for a future refresh.
  - Support for the Power Eraser command.  
Support for this command in the cloud console is slated for a future refresh.
  - Improved AutoUpgrade error reporting.
- Upgraded these third-party components to the following versions:
  - AppRemover 4.3.31.1
  - PHP 7.1.29
  - JDBC 7.2 (for Symantec Endpoint Protection Manager)
  - JRE 1.8u212
  - OpenGC 0.19.0.0
- Removed support for Mac OS X 10.10.
- Removed the full list of system requirements from the release notes PDF. They are now only published on the online page in the knowledge base.

#### [System requirements for Symantec Endpoint Protection 14.2 RU1 MP1](#)

#### [New fixes and component versions in Endpoint Protection 14.2 RU1 MP1](#)

##### **Version 14.2 RU1 MP1 (cloud-managed only)**

*Documentation:* [Symantec Endpoint Security](#)

##### **Version 14.2 RU1 (refresh)**

- Support for kext notarization in macOS 10.14.5  
See: [Endpoint Protection 14.2 RU1 and kext notarization for macOS 10.14.5](#)
- LiveUpdate Support for Web Security Service (WSS) Traffic Redirection content within the Mac client for Symantec Endpoint Protection

No new fixes specific to this refresh. Otherwise, refer to: [New fixes and component versions in Endpoint Protection 14.2 RU1](#)

##### **Version 14.2 RU1**

Symantec Endpoint Threat Defense for Active Directory integration

- Symantec Endpoint Protection delivers a single agent that Endpoint Threat Defense for Active Directory uses when you introduce it into your environment. [Product guides for Symantec Endpoint Threat Defense for Active Directory.](#)
- **Performance improvements for intrusion prevention on servers:** Use a new signature subset for servers to provide a protection profile that is optimized for servers. In addition, Symantec Endpoint Protection introduces a new operational mode option for Intrusion Prevention: Out-of-band scanning. This mode changes the processing model for

---

networking traffic. Symantec recommends that you test out-of-band scanning before you deploy it to your production environment, as performance characteristics vary depending on the workload.

- Simplify deployment of Symantec Endpoint Protection through the addition of support for NT LAN Manager (NTLM) proxy authentication.
- Improved cloud onboarding The links within the Cloud tab of Symantec Endpoint Protection Manager now point directly to the cloud console.
- Support added for Windows 10 May 2019 Update.
- Symantec Advanced Threat Protection (ATP) is now Symantec Endpoint Detection and Response (Symantec EDR).
- All software downloads and licensing details are now available through MySymantec.
- Removed Lotus Notes and Internet Email protection in the Virus and Spyware Protection policy. You can still configure legacy client installation packages with these features through Symantec Endpoint Protection Manager.

#### [New fixes and component versions in Endpoint Protection 14.2 RU1](#)

##### **Version 14.2 RU1 (cloud-managed only)**

*Documentation:* [Symantec Endpoint Security](#)

#### [Upgrading to Symantec Endpoint Security from Symantec Endpoint Protection](#)

##### **Version 14.2 MP1 (refresh)**

- Improvements to Symantec Endpoint Protection Hardening - Application Control and Application Isolation

#### [New fixes and component versions in Endpoint Protection 14.2 MP1](#)

##### **Version 14.2 MP1 (refresh)**

- Support for compatibility with Symantec Endpoint Protection Hardening - Application Control
- REST API enhancements for Symantec Advanced Threat Protection: Endpoint
- Support for the following operating systems:
  - Windows Server 2019
  - Windows 10 October 2018 Update (version 1809), including support for case-sensitivity
  - macOS 10.14 (Mojave)
  - Red Hat Enterprise Linux Server (RHEL) 7U5 (7.5)
  - Support for Linux inode64 and XFS
  - Support for Windows Server 2016 Hyper-V

#### [New fixes and component versions in Endpoint Protection 14.2 MP1](#)

##### **Version 14.2 MP1**

- Support for compatibility with Symantec Endpoint Protection Hardening
- Added support for the following operating systems:
  - Windows Server 2019
  - Windows 10 October 2018 Update (version 1809), including support for case-sensitivity
  - macOS 10.14 (Mojave)
  - Red Hat Enterprise Linux Server (RHEL) 7U5 (7.5)
- Support for Linux inode64 and XFS
- Support for Windows Server 2016 Hyper-V
- Removed support for Windows Server 2008 (RTM) for Symantec Endpoint Protection Manager.
- REST API enhancements for Symantec Endpoint Detection and Response

#### [New fixes and component versions in Endpoint Protection 14.2 MP1](#)

##### **Version 14.2**

---

## Cloud-based features

- **By default, groups and devices are managed by the Symantec Endpoint Protection Manager rather than by the cloud portal:** After you enroll a domain, the Symantec Endpoint Protection Manager manages groups and devices by default. In version 14.1, the cloud portal was the default.
- **Automatically upgrading clients with Symantec Endpoint Protection Hardening:** Symantec Endpoint Protection Hardening was introduced between the 14.0 and the 14.2 releases. As a result, you could not upgrade 14.0.x clients with Symantec Endpoint Protection (SEP) Hardening automatically.
  - In 14.2, you can install Symantec Endpoint Protection Hardening on Windows clients using AutoUpgrade even if the feature was not previously installed. In the client installation package, even if **Maintain existing client features when updating** is checked, you can still install Hardening. You must also make sure that **Application Hardening** is selected in the custom feature set (enabled by default), or else Symantec Endpoint Protection Hardening does not install.
  - 14.2 supports Symantec Endpoint Protection Hardening on both 32-bit and 64-bit Windows desktop operating systems. Earlier clients only support 64-bit Windows desktop operating systems. Symantec Endpoint Protection Hardening is not supported on server operating systems.
- **Support for roaming clients:** Roaming clients intermittently connect to the management server. In 14.2, when the clients cannot connect to the management server, roaming clients automatically send critical events to the cloud portal. After the client reconnects to the management server, the clients send any new critical events to the management server.
- **Integration with the Symantec Content Analysis System:** The Symantec Content Analysis System (CAS) determines how malicious a file is based on its cloud-based file reputation classification service that identifies known files. The service uses reputation scores, numbers (1- 10) to indicate whether files are known to be trusted or malicious. High scores are more likely to be malicious. You can integrate the Symantec Endpoint Protection Manager with the Content Analysis System so that you can submit a file for analysis from the cloud portal to the CAS. After the CAS returns the reputation score, you can take an action on the file, such as blocking it or whitelisting it. To integrate the Symantec Endpoint Protection Manager with the CAS, click the **Admin > Servers > Edit Site Properties > Content Analysis System** tab. To submit files for analysis, go to the cloud portal.
- **Replication for multiple sites available for a management server enrolled in cloud portal:** You can now enroll sites that replicate with partner sites into the cloud portal. The partner site is not enrolled in the cloud portal, but continues to replicate data with the first site.
- **Data collection and submissions options automatically enabled:** After the Symantec Endpoint Protection Manager is enrolled in the cloud portal, the settings for data collection and submissions become automatically enabled. This occurs regardless of whether or not these settings were disabled beforehand. Symantec recommends that you keep these settings enabled so that the clients take advantage of the cloud's AML features.

## Protection features

- **Support for IPv6:** IPv6 support is added for the following items:
  - Communication between Windows, Mac, and Linux clients and the Symantec Endpoint Protection Manager.
  - Communication between the console and the management server, such as logging on locally or remotely to Symantec Endpoint Protection Manager.
  - Communication between management servers and internal LiveUpdate servers that run LiveUpdate Administrator.
  - IPv6-based criteria for many policies, such as custom IPS signatures, location awareness, Group Update Providers, and exceptions.
- The Symantec Endpoint Protection firewall for Mac provides the firewall protection that fully integrates into Symantec Endpoint Protection, which includes events, policies, and commands. You manage and configure the firewall rules

---

and some settings in the same Symantec Endpoint Protection Manager firewall policy as for Windows. The Symantec Endpoint Protection firewall is only available for managed clients.

- **WSS Traffic Redirection for Mac:** WSS Traffic Redirection (WTR) directs web traffic with a Proxy Auto Configuration file URL to Symantec Web Security Service. This traffic redirection secures the web traffic for the client computer. This Symantec Endpoint Protection version extends WSS Traffic Redirection functionality to Macs.
- **WSS Traffic Redirection enhancements for Windows:** This Symantec Endpoint Protection version adds enhanced client authentication for Symantec Web Security Services (WSS). It enables a more granular level of security management for WSS Traffic Redirection. Additionally, you can configure it to forward additional header data that identifies the user that initiated the traffic. This additional header data lets you create per-user traffic rules. To access this setting, click **Policies > Integrations**, open the policy, and click **WSS Traffic Redirection**.
- **Scans quickly handle a large number of threats on heavily infected computers:** When manual scans and Auto-Protect scans detect a large number of threats on a client computer, the scans can quickly process the threats. This aggressive mode starts when the computer has a minimum of 100 viruses. The default action for these detections is Delete. This aggressive mode does not process spyware. You do not configure this feature; it runs automatically.

### Management server features

- **Symantec VIP two-factor authentication and smart card authentication for Symantec Endpoint Protection Manager:** You can now use two additional types of authentication for Symantec Endpoint Protection Manager administrator accounts:
  - **Two-factor authentication (2FA) with Symantec VIP:** When two-factor authentication is enabled, you must provide a unique, one-time verification code as well as a password when you log on to Symantec Endpoint Protection Manager. You can receive the code by voice, text, or with the free Symantec VIP Access application.
  - **Smart card authentication:** You can configure Symantec Endpoint Protection Manager to log on administrators who use a Personal Identity Verification (PIV) card or a Common Access Card (CAC). Smart cards are used for administrators who work for US Federal Agencies or a US military agency. With PIV/CAC authentication, you insert the card into the reader and provide a PIN number.
- **New communications module:** A new communications module replaces the existing protocol. Both modules still use sylink.xml to establish a management connection between Symantec Endpoint Protection Manager and the client. The new communications module works with both IPv6 and IPv4 addresses, and communicates with Windows, Mac, and Linux clients.
- **Password requirements are stronger:** When you install the management server or configure the management server, you must set a strong password for the system administrator account. The password must contain at least 8 characters and fewer than 16 characters. It must include at least one lowercase letter [a-z], one uppercase letter [A-Z], one numeric character [0-9], and one special character ["/ \ [ ] : ; | = , + \* ? < >].
- **Updates for FIPS 140-2 compliance:** Symantec Endpoint Protection 14.2 updates third-party components and validated modules to ensure continued compliance for data encryption with Federal Information Processing Standardization (FIPS) 140-2. Symantec Endpoint Protection 14.2 lets FIPS 140-2-compliant environments access cloud features.
- **LiveUpdate downloads content for the Application Control engine:** To patch problems with an operating system such as Windows 10, LiveUpdate now downloads content for the Application Control engine for 14.2 Windows clients. To access the Application Control content, click **Admin > Edit Site Properties > LiveUpdate tab > Content Types to Download**. You should always keep this option enabled.
- Additional vendors and products are added to the third-Party security software removal feature.

### System requirements

The Symantec Endpoint Protection Manager web console and Help add the following browser support: Mozilla Firefox 5.x through 60.x; Google Chrome 66.x

### Removed, unsupported, or modified features

- **Removed the Host Integrity for Mac option:** Host Integrity policies for Mac required the installation of the Symantec Network Access Control On-Demand client for Mac. Symantec Network Access Control reached End of Life in



---

November 2017, and is not supported for use with Symantec Endpoint Protection 14.x. The Mac option to add a predefined requirement for the Mac client was still in the user interface until 14.2.

- **Removed the Failed Network Compliance Status report:** This report was a Compliance report type that was used for Symantec Network Access Control. You could access the report in the following places:
  - **Reports** page > **Quick Reports** tab > **Compliance report** type
  - **Monitors** page > **Summary** tab > **Summary type** drop-down list
  - **Home** page > **Favorite Reports** section
- **Changes to the third-party security software removal feature:** Changes to the third-party security software removal for version 14.2 mean that you cannot enable it for installation packages for earlier versions. For example, you cannot enable third-party security software removal for version 14.0.1 client packages if you create them with and deploy them from Symantec Endpoint Protection Manager version 14.2.

## Documentation changes

The following options on the **Admin > Administrator** page were changed to be clearer:

- **Attempt Threshold** was changed to **Number of Incorrect Logon Attempts Allowed**
- **Password Verification Attempt Threshold** was changed to **Number of Change Current Password Attempts Allowed**. In addition, this option was described incorrectly. This option displays the number of times you try to change the password on another administrator account, but type the wrong current password.
- **Failed Password Verification Attempts** was changed to **Failed Change Current Password Attempts**.

[New fixes and component versions in Endpoint Protection 14.2](#)

## Version 14.0.1 MP2

### What's new in this version

- Support for Windows 10 April 2018 Update (version 1803)  
(This support is backward-compatible to 14.0.1.)
- Customer defects
- Customer experience
  - Support for Microsoft Storage Spaces
  - Support for Microsoft OneDrive
  - Support for SQL Server databases that are hosted on Amazon RDS
- Third-party component updates

[New fixes and component versions in Endpoint Protection 14.0.1 MP2](#)

## Version 14.0.1 MP1

### Cloud-based features

- **Symantec Endpoint Protection Hardening:** Symantec Endpoint Protection provides application isolation. Application isolation protects users from malicious macros in Microsoft Office, malicious PDF files, and browser plug-ins with vulnerabilities. Application Isolation protects applications from overwrites by other applications if both the applications use same resource. For example, infected tab of a browser may end up sharing the same memory with the other tab. One infected tab may infect the tabs on other browsers. Symantec Endpoint Protection Hardening provides a set of policies that you can use to isolate applications so that they operate in a protected environment.

### Protection features

- **WSS Traffic Redirection:** Symantec Endpoint Protection provides web security to remote users by connecting the client to Web Security Services (WSS) when a route through a corporate network is not possible or practical. WSS Traffic Redirection (WTR) directs traffic from the endpoint to WSS/CASB Services, eliminating the need to install a separate client. You deploy them once and manage them centrally, which lowers the cost of management and

---

eliminates conflict between the agents. This functionality allows Symantec Endpoint Protection to rapidly enable connectivity to cloud services with minimal interruption to users.

- **Ability to test new engine content and definitions before they are released:** Symantec Endpoint Protection contains several content engines that carry out parts of its functionality. Symantec provides a special server that lets you download and test the engine content before you roll out the content to your production environment. Engine updates are released to the EAS for 2 weeks before its phased release on the public LiveUpdate server. Symantec provides the engine updates using your regular LiveUpdate configuration. You can find the option Use a Symantec LiveUpdate early release server in the LiveUpdate Settings policy.
- **Option to lock engine version:** The LiveUpdate Content policy now has the option to revert to an older version of the engine but continue to receive the latest content that corresponds with that engine. In the LiveUpdate Content policy under **Windows Settings**, click **Security Definitions > Select an engine version > Edit**. Clients that are locked to a specific engine version only receive LiveUpdate content that corresponds to that engine version.

### Management server features

On the Symantec Endpoint Protection Manager Home page banner, the **Latest News** link changed to **Latest Alerts**. The associated bell-shaped icon now displays a red dot to indicate new messages. Click **Latest Alerts** to read the news or alerts about Symantec Endpoint Protection.

### System requirements

Added the following support:

- Third-party component upgrades, including Java SE Development Kit 8, zlib, and Commons-Jelly.
- Symantec Endpoint Protection Manager web console: Mozilla Firefox 5.x through 57.x, Google Chrome 63.0.x

### REST API commands

The documentation for the Symantec Endpoint Protection Manager REST APIs is now available in the following locations:

- <http://apidocs.symantec.com/home/saep/> - You can access this location from the cloud portal Help by clicking the last icon at the bottom of the dashboard. Note: If Symantec Endpoint Protection Manager is enrolled with the cloud portal, using REST API commands to manage what the cloud portal manages is not supported.
- On the Symantec Endpoint Protection Manager server at the following address, where SEPM-IP is the IP address of the Symantec Endpoint Protection Manager server: <https://SEPM-IP:8446/sepm/restapidocs.html>

### Removed or unsupported features

- **End-of-Support for Network Access Control:** Symantec discontinued technical support and content updates for customers with current Basic Maintenance Support or Essential Support on November 5, 2017 for Symantec Network Access Control, Symantec Network Access Control Starter Edition, and Symantec Network Access Control Enforcer with 6100 Series Appliance. Host Integrity has already been integrated in Symantec Endpoint Protection.

### [New fixes and component versions in Endpoint Protection 14.0.1 MP1](#)

#### Version 14.0.1 / 14.1

Version 14.01 refers to the client; version 14.1 refers to Symantec Endpoint Protection Manager.

#### What is the difference between the Symantec Endpoint Protection 14.0.1 and 14.1 releases?

Symantec Endpoint Protection 14.0.1 is the next release after version 14 MP2 and includes improvements for both the Symantec Endpoint Protection Manager and the Symantec Endpoint Protection clients. 14.0.1 also includes components to connect to and manage Symantec Endpoint Protection Manager from a new cloud portal that is part of the subsequent release, version 14.1. Version 14.1 releases about the same time as 14.0.1. Symantec Endpoint Protection 14.1 includes the cloud portal, a 14.0.1 Symantec Endpoint Protection Manager, and 14.0.1 clients. The functionality for Symantec Endpoint Protection Manager and the clients does not change, and the user interface for both components is still labeled as 14.0.1. You do not need to upgrade to a new 14.1 management server or new 14.1 clients. The 14.1 cloud portal lets you manage Symantec Endpoint Protection Manager clients and includes some additional functionality that Symantec Endpoint Protection Manager does not have. If you do not enroll in the cloud portal, you continue to manage your client



---

computers entirely from Symantec Endpoint Protection Manager. To connect to the cloud portal, you enroll a 14.0.1 Symantec Endpoint Protection Manager domain in the 14.1 cloud portal.

#### [What's new for Symantec Endpoint Protection \(SEP\) 14.0.1 \(14 RU1\)](#)

For an overview of the new cloud-based features available as of this release, see:

#### [Endpoint Protection 14.1 product tour](#)

#### [New fixes and component versions in Endpoint Protection 14.0.1](#)

#### **Version 14 MP2**

- Third-party component upgrades

#### [New fixes and component versions in Endpoint Protection 14 MP2](#)

#### **Version 14 MP1**

##### **NOTE**

If you run 14 MP1 (14.0.2332.0100), DO NOT upgrade to the 14 MP1 Refresh Build (14.0.2349.0100). Both versions are considered current. Upgrading from 14 MP1 to 14 MP1 Refresh Build (14.0.2349.0100) is NOT supported. The code change in 14 MP1 Refresh Build, which addresses the following issue, is slated for inclusion in a future release of version 14:

[Using a sole trailing backslash with an Exception prefix variable in SEP 14 MP1 causes ccSvcHst.exe to crash](#)

- Support for Red Hat Enterprise Linux (RHEL) 7.3.
- Third-party components updates, including PHP, Java, and Apache Tomcat.
- Corrected style and formatting issues within the Symantec Endpoint Protection Manager user interface.

#### [New fixes and component versions in Endpoint Protection 14 MP1](#)

#### **Version 14**

- **Improved protection:**
  - Virus definitions in the cloud (Intelligent Threat Cloud Service)
  - Advanced Machine Learning (AML) on the endpoint for improved static detections
  - OS hardening (Generic Exploit Mitigation)
  - Emulator for packed malware
  - Security patches for Windows clients that download using LiveUpdate
- **Usability and scale:**
  - New user interface
  - Custom replication schedule
  - Subnet mask for explicit Group Update Providers
  - In-product notifications
  - REST API references
- **Cross-platform support:**
  - Device control (Mac client)
  - AutoUpgrade (Mac client)

#### **System requirements**

For the full list of system requirements, see [System requirements for Symantec Endpoint Protection 14](#).

- *Symantec Endpoint Protection Manager:*
  - Support added for Windows Server 2016
- *Windows client:*

- 
- Support added for Windows 10 Anniversary Update
  - *Linux client:*
    - Support added for Red Hat Enterprise Linux (RHEL) 7.1 and 7.2 (precompiled binary support)
    - Support added for Oracle Linux (OEL) 6U5
  - *Mac client:*
    - Support added for macOS 10.12 (Sierra)
  - *Database:*
    - Support added for SQL Server 2014 SP2
  - Browser support for the Symantec Endpoint Protection Manager web console and Help:
    - Microsoft Edge
    - Mozilla Firefox 5.x through 49.0.1
    - Google Chrome through 54.0.x

[What's new in Symantec Endpoint Protection \(SEP\) 14](#)

[New fixes and component versions in Endpoint Protection 14](#)

## What's new for Symantec Endpoint Protection 14.3 RU1 MP1

This section describes the new features in this release.

### 14.3 RU1 MP1

- Added ability to log in to Symantec Endpoint Protection Manager using credentials in AD format (i.e. username@domain.com or domain\username).
- Added ability to sync usernames in both formats from Active Directory (UserPrincipalName and pre-Windows 2000 logon name - sAMAccountName). Symantec Endpoint Protection Manager no longer creates duplicate entries and handles both usernames as expected.
- The new option **Maintain existing client features when updating** under **Installation Features and Settings** lets you create and export a client package that will only upgrade the client to a new version but will make no changes to the configuration, client communication, or installed features.
- Antimalware AMSI Scan now takes the file/folder exceptions into account when scanning a script file before it runs.
- Added ability to sync macOS details from Active Directory.
- More information in logs:
  - Log entries contain full client group information.
  - The Live Update events contain the revision information.
- The database schema includes the following table changes:
  - New column "user\_name\_2" added in the SEM\_CLIENT table.

## What's new for Symantec Endpoint Protection 14.3 RU1?

This section describes the new features in this release.

### Protection Features

- Includes the new Symantec Mac Agent and the Symantec Linux Agent that can be installed and managed from either the on-premises Symantec Endpoint Protection Manager or the Integrated Cyber Defense Manager cloud console.  
[Installing the Symantec Endpoint Protection client for Mac](#)  
[Installing the Symantec Agent for Linux 14.3 RU1](#)
- Prevents new and unknown threats on the macOS by monitoring file behaviors in real time. The new Mac Agent includes these behavioral protection capabilities. Behavioral protection, or SONAR, uses artificial intelligence and advanced machine learning for zero-day protection to effectively stop new threats.

---

## Managing SONAR

- Blocks untrusted non-portable executable (PE) files such as PDF files and scripts (such as PowerShell, JavaScript, and VBScript) that are not yet identified as a threat. In the Exceptions policy, click **Windows Exceptions > File Access**.
- Prevents web threats based on the reputation score of a web page. The Intrusion Prevention policy includes URL reputation filtering, which blocks web pages with reputation scores below a specific threshold. Reputation scores range from -10 (bad) to +10 (good). The **Enable URL Reputation** option is enabled by default.
- You can force Symantec Endpoint Protection to learn an application based on the application's hash value. In the Exceptions policy, click **Windows Exceptions > Application > Add an Application by Fingerprint**.
- Protects endpoints and users from web-based attacks on malicious sites using the Network Traffic Redirection feature. Network Traffic Redirection redirects all network traffic (any port) or just web-based traffic (ports 80 and 443) to the Symantec Web Security Service, which allows or blocks network traffic and SaaS application access based on the enterprise policy. The Network Traffic Redirection policy has a new redirection method called the tunnel method. The tunnel method automatically redirects all Internet traffic to the Symantec WSS, where the traffic is allowed or blocked based on the Symantec Web Security Service policies. The tunnel method is considered an early adopter release feature. You should perform thorough testing with your applications against your WSS policies.

## Configuring Network Traffic Redirection

- The Integrations policy was renamed to the Network Traffic Redirection policy.
- Provides support for MITRE-enriched events in Symantec EDR. Leverage the MITRE ATT&CK framework to provide context into what is happening in your environment.
- Provides support for the following Symantec EDR events, which expose more visibility into the endpoints:
  - AMSI events provide visibility of threat actor methods that can evade traditional command-line interrogation methods.
  - ETW events provide visibility into events happening on managed Windows endpoints.
- Includes the ability to run both the Windows Defender and Symantec Endpoint Protection on the same computer. The Auto-Protect scan runs after Windows Defender and can detect any threats that Windows Defender misses. The **Coexist with Windows Defender** option ensures that Auto-Protect runs in case Microsoft Defender is disabled. To disable the option, click the Virus and Spyware Protection policy > **Miscellaneous > Miscellaneous** tab.
- Attack chain mitigation is now supported for hybrid-managed clients.

## Symantec Endpoint Protection Manager

- The embedded database was updated to the Microsoft SQL Express database. The SQL Server Express database stores policies and security events more efficiently than the default embedded database and is installed automatically with the Symantec Endpoint Protection Manager.
- [Best practices for upgrading from the embedded database to the Microsoft SQL Server Express database](#)
- During the installation or upgrade of the Symantec Endpoint Protection Manager, the Management Server Configuration wizard:
    - Automatically installs LiveUpdate content.
    - Provides an option to use TLS certificate for secure communication between SQL Server and the Symantec Endpoint Protection Manager.
  - LiveUpdate uses a new engine in Symantec Endpoint Protection Manager, which is optimized to run on the cloud console. The new engine no longer supports the FTP method or LAN method to specify an internal LiveUpdate server to download content to the Symantec Endpoint Protection Manager.

## Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager

- The **Automatically uninstall existing third-party security software** option that was not available in 14.3 MP1 is available again in 14.3 RU1 with an updated version. This option is used to uninstall third-party security software. To access this option, click **Admin** page > **Packages > Client Install Settings**.

## Third-party security software removal in Endpoint Protection 14

---

### Third-party security software removal in Endpoint Protection 14.3 RU1

- The Client Deployment Wizard that is used to deploy client packages must have its credentials verified and able to connect to the Symantec Endpoint Protection Manager. If the verification process fails, the client deployment process stops to keep Active Directory user accounts from being locked.

### Installing Symantec Endpoint Protection clients with Remote Push

- The Computer Status logs and reports now lets you select a range for the **Client version** and **IPS version** fields. The **Product version** filter was renamed to **Client version**.
- The **Disable the notification tray icon** option is available for clients that run on a terminal server and that cause high CPU usage and memory usage. You can now disable the notification area icon, also known as the system tray icon, to prevent multiple instances of user session processes (like SmcGui.exe and ccSvcHost.exe) from running. For clients that run on a terminal server, the **Disable the notification area icon** option overrides the registry key setting in HKLM\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\LaunchSMCGui. In lieu of manually changing this key, it is now managed via policy. As a best practice, move clients that are on a terminal server in the same group before you upgrade. For clients that do not run on a terminal server, keep this setting disabled. This option takes place only after the client smc service is restarted. You enable this option on the **Clients > Policies** tab > **General > General Settings** tab.
- Updated the whitelist and blacklist mode to reflect the allow and block functionality. On the **Clients** page > **Policies** tab > **System Lockdown** dialog box, the application file lists changed from **Whitelist Mode** and **Blacklist Mode** to **Allow Mode** and **Deny Mode**.
- On the **Admin** page > **Servers** tab > **Configure External Logging > General** tab, the **Master Logging Server** option changed to **Primary Logging Server**.
- The **System** log type > **Administrative** log and the **Audit** log lists the computer name.
- Client firewall logs are collected so that you get fewer notifications on the cloud console.
- Replaced the Oracle Java SE with the OpenJDK.
- Updated the third-party components JQuery to a newer version.

### Client and platform updates

- The Windows client supports Windows 10 20H2 (Windows 10 version 2009).
- The Mac client supports macOS 11 (Big Sur) on a Intel Core i5 processor and later.
- Moved the legacy Mac client installation packages to the AdditionalPackages folder.

### Features Removed

- The **Risk severity** and **Risk Distribution by Severity** options were removed from notifications and reports.
- The **CASMA** tab and **Analyze** command were removed, as this functionality was deprecated in 14.3.
- The Mac client no longer supports macOS 10.13 or 10.14.x.
- You can no longer view exclusions in the registry. For 14.3 RU1 and earlier, to view exclusions, see: [Verify if an Endpoint Client has Automatically Excluded an Application or Directory](#)

### Documentation

The Symantec Endpoint Protection Manager Help is now online and located at: [Symantec Endpoint Protection Installation and Administration Guide](#)

### Database schema

The database schema has the following changes.

Table	Column change
ALERTS	Added the ENRICHED_DATA column.
AGENT_BEHAVIOR_LOG1 AGENT_BEHAVIOR_LOG2 AGENT_PACKET_LOG_1 AGENT_PACKET_LOG_2 AGENT_SECURITY_LOG_1 AGENT_SECURITY_LOG_2 AGENT_SYSTEM_LOG_1 AGENT_SYSTEM_LOG_2 AGENT_TRAFFIC_LOG_1 AGENT_TRAFFIC_LOG_2 BASIC_METADATA COMMAND COMPUTER_APPLICATION ENFORCER_CLIENT_LOG_1 ENFORCER_CLIENT_LOG_2 ENFORCER_SYSTEM_LOG_1 ENFORCER_SYSTEM_LOG_2 ENFORCER_TRAFFIC_LOG_1 ENFORCER_TRAFFIC_LOG_2 IDENTITY_MAP LAN_DEVICE_DETECTED LAN_DEVICE_EXCLUDED LEGACY_AGENT LOCAL_METADATA LOG_CONFIG REPORTS SEM_APPLICATION SEM_CLIENT SEM_COMPUTER SEM_JOB SEM_SVA_CLIENT SEM_SVA_COMPUTER SERVER_ADMIN_LOG_1 SERVER_ADMIN_LOG_2 SERVER_CLIENT_LOG_1 SERVER_CLIENT_LOG_2	Removed the following columns from each table: RESERVED_INT1 RESERVED_INT2 RESERVED_BIGINT1 RESERVED_BIGINT2 RESERVED_CHAR1 RESERVED_CHAR2 RESERVED_VARCHAR1 RESERVED_BINARY

Table	Column change
SERVER_ENFORCER_LOG_1 SERVER_ENFORCER_LOG_2 SERVER_POLICY_LOG_1 SERVER_POLICY_LOG_2 SERVER_SYSTEM_LOG_1 SERVER_SYSTEM_LOG_2 SYSTEM_STATE V_AGENT_BEHAVIOR_LOG V_AGENT_PACKET_LOG V_AGENT_SECURITY_LOG V_AGENT_SYSTEM_LOG V_AGENT_TRAFFIC_LOG V_DOMAINS V_ENFORCER_CLIENT_LOG V_ENFORCER_SYSTEM_LOG V_ENFORCER_TRAFFIC_LOG V_GROUPS V_LAN_DEVICE_DETECTED V_LAN_DEVICE_EXCLUDED V_SEM_COMPUTER V_SERVER_ADMIN_LOG V_SERVER_CLIENT_LOG V_SERVER_ENFORCER_LOG V_SERVER_SYSTEM_LOG V_SERVERS	(Continued)
BINARY_FILE SERVER_POLICY_LOG_1 SERVER_POLICY_LOG_2 V_SERVER_POLICY_LOG	<ul style="list-style-type: none"> <li>• The CONTENT column changed its type from 'image' to 'varbinary'</li> <li>• Added an FILESTREAM_ID indexed column</li> <li>• Added a FILESTREAM_ID index</li> <li>• Removed the following columns:               <ul style="list-style-type: none"> <li>– RESERVED_INT1</li> <li>– RESERVED_INT2</li> <li>– RESERVED_BIGINT1</li> <li>– RESERVED_BIGINT2</li> <li>– RESERVED_CHAR1</li> <li>– RESERVED_CHAR2</li> <li>– RESERVED_VARCHAR1</li> <li>– RESERVED_BINARY</li> </ul> </li> </ul>
INVENTORYREPORT	Added the following columns: <ul style="list-style-type: none"> <li>• PRODUCTVERSIONFROM</li> <li>• PRODUCTVERSIONTO</li> <li>• IDS_VERSIONFROM</li> <li>• IDS_VERSIONTO</li> </ul>

Table	Column change
SEM_AGENT	<ul style="list-style-type: none"> <li>Added the NTR_MESSAGE column.</li> <li>Removed the following columns: <ul style="list-style-type: none"> <li>RESERVED_INT1</li> <li>RESERVED_INT2</li> <li>RESERVED_BIGINT1</li> <li>RESERVED_BIGINT2</li> <li>RESERVED_CHAR1</li> <li>RESERVED_CHAR2</li> <li>RESERVED_VARCHAR1</li> <li>RESERVED_BINARY</li> </ul> </li> </ul>
SEM_AGENT_VERSION	<p>Added the following columns:</p> <ul style="list-style-type: none"> <li>VERSION</li> <li>FORMATTED_VERSION</li> <li>REFRESH_USN</li> <li>AGENT_VERSION_FORMAT_REFRESH</li> <li>VERSION1</li> <li>ntec.com/sep/14/whats_new_all</li> <li>VERSION2</li> <li>VERSION3</li> <li>VERSION4</li> </ul>
SEM_SVA	<p>Removed the following columns:</p> <ul style="list-style-type: none"> <li>RESERVED_INT1</li> <li>RESERVED_INT2</li> <li>RESERVED_BIGINT1</li> <li>RESERVED_BIGINT2</li> <li>RESERVED_CHAR1</li> <li>RESERVED_CHAR2</li> <li>RESERVED_VARCHAR1</li> </ul>
V_ALERTS	Added the ENRICHED_DATA column.

[What's new in all releases of Symantec Endpoint Protection](#)

## What's new for Symantec Endpoint Protection 14.3 MP1 (14.3.0.1)

This section describes the new features in this release.

### 14.3 MP1 (refresh):

Added support with Google Cloud Platform for cloud-enrolled Symantec Endpoint Protection Managers and cloud-managed Symantec Agents. You do not need to upgrade if you continue to use the on-premises Symantec Endpoint Protection Manager to entirely manage your clients. See: [FAQ: Migration of Symantec Endpoint Protection to Google Cloud Platform](#)

### 14.3 MP1:

- A REST API enhancement lets you copy over settings in the **General Settings** policy to other groups. If you do not have inheritance for groups enabled, you can use the API call to change settings for multiple groups. For example, you

---

can set the heartbeat and download randomization values, enable Tamper Protection, and configure Server control options.

- External Logging adds a new Syslog entry containing PII filtered policy changes. This change adds a second log line containing the policy payload when a policy change is made and recorded in the Audit log.
- External Logging forwards information about the type of scan to Syslog servers. This information includes whether the scan was a full scan or active scan and a manual or scheduled scan. This change adds a new SCAN\_TYPE column in External Logging for scan events. You can use this information to track regularly scheduled scans on your client computers.
- The Symantec Endpoint Protection Manager Administrative Log displays the administrator's user name and the source and destination group names after a client moves from one group to another.
- Added command-line scan support for the Windows Subsystem for Linux (WSL) processes. Dependent on SDS 1.12 or later.

#### [What is the Windows Subsystem for Linux?](#)

- The database schema includes the following table changes:
  - SEM\_AGENT: TDAD\_GLOBAL\_DATA\_PROCESSING\_DONE\_TIME (Timestamp for when the agent is done processing the TDAD policy).
  - SERVER\_POLICY\_LOG\_1 and 2: EVENT\_CONTENT (Stores the policy contents when added, edited, or deleted after Audit Log option is enabled.)

## What's new for Symantec Endpoint Protection 14.3?

This section describes the new features for the 14.3 release.

### Protection Features

- Third-party application developers can protect their customers from dynamic script-based malware and from non-traditional avenues of cyberattack. The third-party application calls the Windows AMSI interface to request a scan of user-provided script, which is routed to the Symantec Endpoint Protection client. The client responds with a verdict to indicate on whether or not the script behavior is malicious. If the behavior is not malicious, then the script execution proceeds. If the script's behavior is malicious, the application does not run it. On the client, the Detection Results dialog box displays a status of "Access Denied." Examples of third-party scripts include Windows PowerShell, JavaScript, and VBScript. Auto-Protect must be enabled. This functionality works for Windows 10 and later computers.

[How the Antimalware Scan Interface \(AMSI\) helps you defend against malware](#)

[Antimalware Scan Interface \(AMSI\)](#)

### Symantec Endpoint Protection Manager

- The Symantec Endpoint Protection remote console now supports Java 11 instead of Java 8. To access the remote console, open a supported web browser and type the following address in the address box: `http://SEPMServer:9090/symantec.html` and download new remote console package. Follow the instructions mentioned. The previous version of the Symantec Endpoint Protection Manager remote console is no longer supported.

[Logging on to Symantec Endpoint Protection](#)

- You can configure one of the Symantec Endpoint Protection Managers on the site as a master logging server to forward logs to the syslog server. If the master logging server goes offline, a second management server takes over and forwards logs to the syslog server. When the master logging server comes back online, it resumes forwarding the logs.

[Configuring a failover server for external logging](#)

- The Integrations policy has a new option for WSS Traffic Redirection, **Enable LPS Custom PAC file**. This option lets you replace the default PAC file that is hosted by the LPS server on the client with a custom PAC file. The custom PAC



---

file solves compatibility issues with third-party applications that do not work with a local proxy server listening on the loopback adapter.

- Support for the Microsoft SQL Server 2019 database.
- The antivirus scan process now uses a separate service from the main non-security service. This new scan process brings more efficient memory usage, continual protection, and less dependency on issues with the main service.

#### [Endpoint Protection 14.3 scan process separation](#)

- The database schema includes new columns as part of a feature for a future release. (AGENT\_SECURITY\_LOG\_1, AGENT\_SECURITY\_LOG\_2, SEM\_AGENT tables)
- The Rest API has the following fields in the /sepm/api/v1/computers API response JSON to call and download the Computer Status report: quarantineStatus, quarantineCode, wssStatus, pskVersion.
- Upgraded the following third-party components to newer versions: Apache Tomcat, Boost C++ Libraries, cURL, Jackson-core, jackson-databind, Jakarta Activation, Java, logback, Microsoft JDBC Driver for SQL Server, OpenSC, OpenSSL, Spring Security, spring-framework, sqlite.
- To enroll the Symantec Endpoint Protection Manager domain in the cloud console, you must first get the enrollment token through the Symantec Endpoint Security console. Previously, you got the enrollment token by clicking **Get Started** on the **Cloud** page.

#### **Client and platform updates**

- The Windows client supports Windows 10 20H1 (Windows 10 version 2004)
- The Linux client now supports Ubuntu 18.04, RHEL 8, and CentOS 8.
- The AppRemover tool was updated to a newer version. The AppRemover tool removes third-party applications before you can install the Windows client. For more information on which applications it removes, see: [Third-party security software removal in Endpoint Protection 14.3](#)

#### **Features Removed**

- The following notifications no longer show the **Risk severity** and **Risk type** fields: Risk Outbreak, Single Risk Event, New Risk Detected.

#### [What's new in all releases of Symantec Endpoint Protection](#)

---

# What is Symantec Endpoint Protection?

---

Learn about the Symantec Endpoint Protection architecture and components

Symantec Endpoint Protection is a client-server solution that protects laptops, desktops, and servers in your network against malware, risks, and vulnerabilities. Symantec Endpoint Protection combines virus protection with advanced threat protection to proactively secure your client computers against known and unknown threats, such as viruses, worms, Trojan horses, and adware. Symantec Endpoint Protection provides protection against even the most sophisticated attacks that evade traditional security measures, such as rootkits, zero-day attacks, and spyware that mutates.

Providing low maintenance and high power, Symantec Endpoint Protection communicates over your network to automatically safeguard both physical systems and virtual systems against attacks. Symantec Endpoint Protection provides management solutions that are efficient and easy to deploy and use.

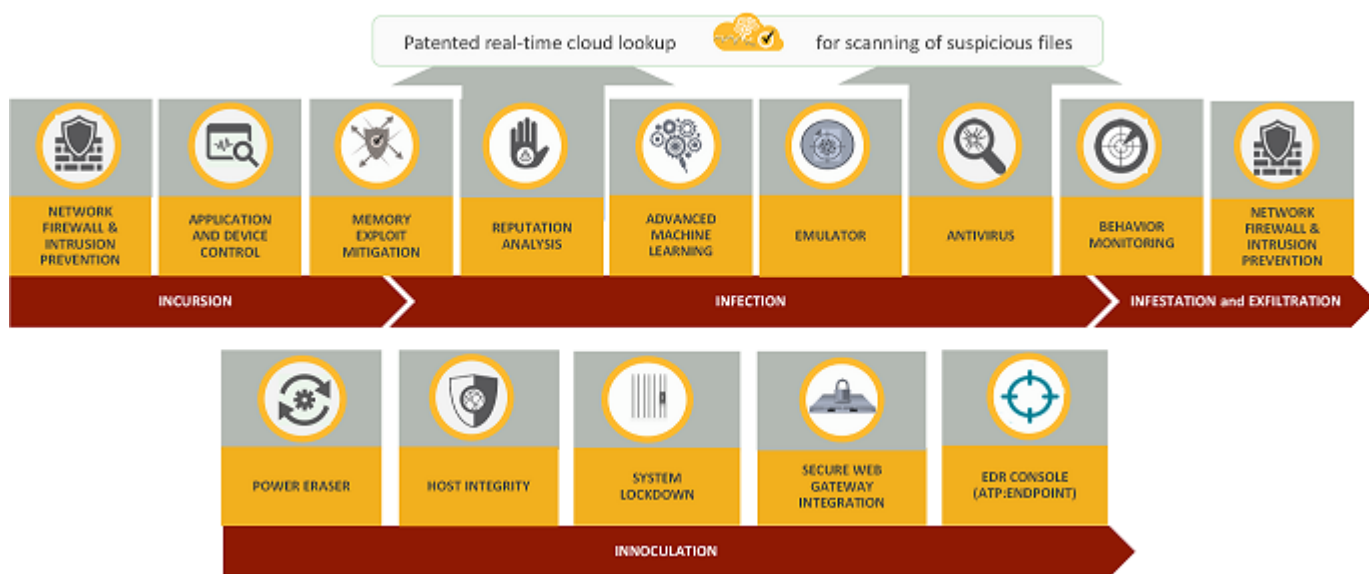
[How Symantec Endpoint Protection technologies protect your computers](#)

[Symantec Endpoint Protection architecture components](#)

## How Symantec Endpoint Protection technologies protect your computers

Symantec Endpoint Protection's core protection against known and unknown threats uses a layered approach to defense. The comprehensive approach protects the network before, during, and after an attack. Symantec Endpoint Protection reduces your risk of exposure by providing tools to increase your security posture ahead of any attack.

To get complete protection for the computers in your network, enable all protections at all times.



[What types of attacks do Symantec Endpoint Protection technologies protect against?](#)

Symantec Endpoint Protection uses the following holistic security approach to protect your environment across the entire attack chain, using the following stages: incursion, infection, infestation and exfiltration, and remediation and inoculation.

### Phase 1: Incursion

---

During the incursion phase, hackers typically break into the organization's network using target attacks such as social engineering, zero-day vulnerabilities, SQL injection, targeted malware, or other methods.

**Symantec Endpoint Protection protects against attacks before they enter your system using the following technologies:**

- **Intrusion Prevention/Firewall (Network Threat Protection):** Analyzes all incoming traffic and outgoing traffic and offers browser protection to block such threats before they can be executed on the computer. The rules-based firewall and browser protection protect against web-based attacks.  
[Managing intrusion prevention](#)  
[Managing firewall protection](#)
- **Application Control:** Controls the file access and registry access and how processes are allowed to run.  
[About application control, system lockdown, and device control](#)  
[Setting up application control](#)
- **Device Control:** Restricts the access to select hardware and control what types of devices can upload or download information.  
[Managing device control](#)
- **Memory Exploit Mitigation:** Neutralizes zero-day exploits like Heap Spray, SEHOP overwrite, and Java exploits in popular software that the vendor has not patched.  
[Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy](#)
- **Web and Cloud Access Protection:** Controls network traffic over all ports and protocols, regardless of where enterprise users are.  
[Configuring Web and Cloud Access Protection](#)

## Phase 2: Infection

In targeted attacks, hackers typically break into the organization's network using social engineering, zero-day vulnerabilities, SQL injection, targeted malware, or other methods.

**Symantec Endpoint Protection uses the following technologies to detect and prevent these attacks before they infect your system:**

- **Memory Exploit Mitigation:** Detects malware.
- **File reputation analysis (Insight):** Based on the artificial intelligence that uses Symantec's global intelligence network. This advanced analysis examines billions of correlated linkages from users, websites, and files to identify and defend against rapidly-mutating malware. By analyzing key attributes (such as the origin point of a file download ), Symantec can accurately identify whether a file is good or bad and assign a reputation score all before the file arrives on the client computer.  
[Managing Download Insight detections](#)
- **Advanced machine learning:** Analyzes the trillions of examples of the good files and bad files that are contained in a global intelligence network. Advanced machine learning is a signatureless technology that can block new malware variants at the pre-execution.  
[How does Symantec Endpoint Protection use advanced machine learning?](#)
- **High-speed emulation:** Detects hidden malware using polymorphic custom packers. A scanner runs each file in milliseconds in a lightweight virtual machine that causes threats to reveal themselves, improving both the detection rates and performance.  
[How does the emulator in Symantec Endpoint Protection detect and clean malware?](#)
- **Antivirus file protection (Virus and Spyware Protection):** Uses signature-based antivirus and file heuristics to look for and eradicate malware on a system to protect against viruses, worms, Trojans, spyware, bots, adware, and rootkits.  
[Managing scans on client computers](#)  
[About the types of scans and real-time protection](#)
- **Behavioral monitoring (SONAR):** Leverages machine learning to provide zero-day protection, stopping new and unknown threats by monitoring nearly 1,400 file behaviors while they execute in real time to determine file risk.

### Phase 3: Infestation and Exfiltration

Data exfiltration is the unauthorized transfer of data from a computer. Once the intruders control these target systems, they may steal intellectual property or other confidential data. Attackers use captured information for analysis and further exploitation or fraud.

- **Intrusion Prevention/Firewall:** Block threats as they travel through the network.
- **Behavioral monitoring:** Helps stop the spread of infection.

### Phase 4: Remediation and Inoculation

Symantec Endpoint Protection includes a single console and agent that offers protection across operating systems, platforms, and businesses of any size.

- **Power Eraser:** An aggressive tool, which can be triggered remotely, to address advanced persistent threats and remedy tenacious malware.  
[What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console](#)
- **Host Integrity:** Ensures that endpoints are protected and compliant by enforcing policies, detecting unauthorized changes, and conducting damage assessments. Host Integrity then isolates a managed system that does not meet your requirements.  
[How Host Integrity works](#)
- **System Lockdown:** Allows applications (that are known to be good) to run, or blocks the applications (known to be bad) from running. In either mode, System Lockdown uses checksum and file location parameters to verify whether an application is approved or unapproved. System Lockdown is useful for kiosks where you want to run a single application only.  
[Configuring system lockdown](#)
- **Secure Web Gateway Integration:** Uses programmable REST APIs to make integration possible with Secure Web Gateway, to help quickly stop the spread of infection at the client computer.
- **EDR Console Integration.** Symantec Endpoint Protection is integrated with Symantec Endpoint Detection and Response and is designed to detect, respond, and block targeted attacks and advanced persistent threats faster by prioritizing attacks. EDR (Endpoint Detection and Response) capability is built into Symantec Endpoint Protection, which makes it unnecessary to deploy additional agents.  
[Configuring system lockdown](#)

### What types of attacks do Symantec Endpoint Protection technologies protect against?

The following table displays which types of Symantec Endpoint Protection technologies protects against which types of attacks.

**Table 15: What types of attacks does each Symantec Endpoint Protection technology protect against?**

Attack	Advanced machine learning	Heuristics	Intrusion Prevention	Network Protection	Policy lockdown
Zero-day	√	√	√		√
Social engineering	√	√	√	√	√
Ransomware	√	√		√	√
Targeted attack	√	√	√		√
Advanced persistent threat	√	√	√		
Drive-by download		√	√		

## Symantec Endpoint Protection architecture components

The Symantec Endpoint Protection architecture uses three functional groups of components. Some of the components belong in multiple groups because they are multi-functional.



Table 16: Main components

Component	Description
Symantec Endpoint Protection Manager	<p>Symantec Endpoint Protection Manager is a management server that manages events, policies, and client registration for the client computers that connect to your company's network.</p> <p>Symantec Endpoint Protection Manager includes the following subcomponents:</p> <ul style="list-style-type: none"><li>The management server software provides secure communication to and from the client computers and the console.</li><li>The console is the interface to the management server. The console software coordinates and manages security policies, client computers, reports, logs, roles and access, administrative functions, and security. You can also install a remote console and use it to log on to the management server from any computer with a network connection.</li><li>The database stores security policies and events and is installed with Symantec Endpoint Protection Manager. You can also install a Microsoft SQL Server database to use instead of the automatically installed Microsoft SQL Server Express (as of 14.3 RU1) or embedded database (14.3 MP1 and earlier). SQL Server is recommended for larger organizations with 5000+ computers. Symantec Endpoint Protection Manager communicates with either a local or remote Microsoft SQL Server database.</li></ul> <p><a href="#">Installing Symantec Endpoint Protection Manager</a></p>
Symantec Endpoint Protection client	<p>The Symantec Endpoint Protection client provides the security protection part of the solution. The client downloads policies and sometimes content from the Symantec Endpoint Protection Manager and runs on Windows, Mac, and Linux.</p>

Symantec Endpoint Protection enables a client to download content from the management server, Group Update Provider, an Internal LiveUpdate server, or the Internet.

**Table 17: Optional components and their functions**

Component	Description
LiveUpdate Administrator	<p>LiveUpdate Administrator downloads definitions, signatures, and other content from an internal LiveUpdate server and distributes the updates to client computers. You can use an internal LiveUpdate server in very large networks to reduce the load on the Symantec Endpoint Protection Manager. You should also use the internal LiveUpdate server if your organization runs multiple Symantec products that also use LiveUpdate to update client computers.</p> <p>You can get LiveUpdate Administrator from <a href="#">Download LiveUpdate Administrator (LUA)</a>.  <a href="#">Choose a distribution method to update content on clients</a>  <a href="#">Configuring clients to download content from an internal LiveUpdate server</a></p>
Group Update Provider (GUP)	<p>The Group Update Provider helps distribute content within the organization, particularly useful for groups at remote locations with minimal bandwidth. Organizations that have a lot of clients may want to use Group Update Providers (GUPs) for Windows clients. GUPs reduce the load on the management server and are easier to set up than an internal LiveUpdate server.</p> <p><a href="#">Using Group Update Providers to distribute content to clients</a></p>
Symantec Endpoint Security cloud console	<p>Symantec Endpoint Security is the management console that you use to manage client computers from the cloud. Symantec Endpoint Security is the fully cloud-managed version of the on-premises Symantec Endpoint Protection. You can manage computers from any one of the following options:</p> <ul style="list-style-type: none"> <li>• Symantec Endpoint Protection Manager (on-premises only)</li> <li>• From Symantec Endpoint Protection Manager and Symantec Endpoint Security (hybrid: on-premises and cloud)  <a href="#">Enrolling a domain in the cloud console from the Symantec Endpoint Protection Manager console</a></li> <li>• Symantec Endpoint Security (cloud only)  <a href="#">Upgrading to Symantec Endpoint Security from Symantec Endpoint Protection</a></li> </ul> <p>Symantec Endpoint Security runs on the Symantec Integrated Cyber Defense Manager (ICDm), the cloud platform that unifies cloud and on-premises products in one place.</p>

Symantec Endpoint Protection also comes with multiple tools to help you increase security and manage the product.

[What are the tools included with Symantec Endpoint Protection?](#)

[How Symantec Endpoint Protection technologies protect your computers](#)

---

# Getting Started

---

Get up and running immediately on Symantec Endpoint Protection

Assess your security requirements and decide if the default settings provide the balance of performance and security that you require. Some performance enhancements can be made immediately after you install Symantec Endpoint Protection Manager.

Perform the following tasks to install and protect the computers in your network immediately:

- [Step 1: Plan your installation structure](#)
- [Step 2: Prepare for and then install Symantec Endpoint Protection Manager](#)
- [Step 3: Add groups, policies, and locations](#)
- [Step 4: Change communication settings to increase performance](#)
- [Step 5: Activate the product license](#)
- [Step 6: Decide on a client deployment method](#)
- [Step 7: Prepare the client for installation](#)
- [Step 8: Deploy and install the client software](#)
- [Step 9: Check that the computers are listed in the groups that you expected and that the clients communicate with the management server](#)

[What do I do after I install the management server?](#)

## Step 1: Plan your installation structure

Before you install the product, consider the size and geographical distribution of your network to determine the installation architecture.

To ensure good network and database performance, you need to evaluate several factors. These factors include how many computers need protection, whether any of those computers connect over a wide-area network, or how often to schedule content updates.

- If your network is small, is located in one geographic location, and has fewer than 500 clients, you need to install only one Symantec Endpoint Protection Manager.
- If the network is very large, you can install additional sites with additional databases and configure them to share data with replication. To provide additional redundancy, you can install additional sites for failover or load balancing support. Failover and load balancing can only be used with Microsoft SQL Server databases.
- If your network is geographically dispersed, you may need to install additional management servers for load balancing and bandwidth distribution purposes.

To help you plan medium to large-scale installations, see: [Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper](#).

[Network architecture considerations](#)

[Setting up sites and replication](#)

[Setting up failover and load balancing](#)

## Step 2: Prepare for and then install Symantec Endpoint Protection Manager

1. Make sure the computer on which you install the management server meets the minimum system requirements.  
See: [Release notes, new fixes, and system requirements for all versions of Endpoint Protection](#)
2. To install Symantec Endpoint Protection Manager, you must be logged on with an account that grants local administrator access.

- 
3. Decide on whether to use the default Microsoft SQL Server Express database or a Microsoft SQL Server database. If you use a Microsoft SQL Server database, the installation requires additional steps. These include, but are not limited to, configuring or creating a database instance that is configured to use mixed mode or Windows authentication mode. You also need to provide database server administration credentials to create the database and the database user. These are specifically for use with the management server.

[About SQL Server configuration settings](#)

[Setting up failover and load balancing](#)

4. You install Symantec Endpoint Protection Manager first. After you install, you immediately configure the installation with the Management Server Configuration Wizard.

Decide on the following items when you configure the management server:

- A password for your logon to the management console
- An email address where you can receive important notifications and reports
- An encryption password, which may be needed depending on the options that you select during installation

[Installing Symantec Endpoint Protection Manager](#)

[About basic management server settings](#)

[Configuring Symantec Endpoint Protection Manager after installation](#)

### Step 3: Add groups, policies, and locations

1. You use groups to organize the client computers, and apply a different level of security to each group. You can use the default groups, import groups if your network uses Active Directory or an LDAP server, or add new groups.

If you add new groups, you can use the following group structure as a basis:

- Desktops
- Laptops
- Servers

[Importing existing groups and computers from an Active Directory or an LDAP server](#)

[How you can structure groups](#)

[Adding a group](#)

2. You use locations to apply different policies and settings to computers based on specific criteria. For example, you can apply different security policies to the computers based on whether they are inside or outside the company network. In general, the computers that connect to your network from outside of your firewall need stronger security than those that are inside your firewall.

A location can allow the mobile computers that are not in the office to update their definitions automatically from Symantec's LiveUpdate servers.

See [Best Practices for Symantec Endpoint Protection Location Awareness](#) .

[Adding a location to a group](#)

3. Disable inheritance for the groups or locations for which you want to use different policies or settings. By default, groups inherit their policies and settings from the default parent group, **My Company**. If you want to assign a different policy to child groups, or want to add a location, you must first disable inheritance. Then you can change the policies for the child groups, or you can add a location.

#### NOTE

Symantec Endpoint Protection Manager policy inheritance does not apply to the policies that are received from the cloud. The cloud policies follow the inheritance as defined in the cloud.

[Disabling a group's inheritance](#)

4. For each type of policy, you can accept the default policies, or create and modify new policies to apply to each new group or location. You must add requirements to the default Host Integrity policy for the Host Integrity check to have an effect on the client computer.

### Step 4: Change communication settings to increase performance



---

**You can improve network performance by modifying the following client-server communication settings in each group:**

- Use pull mode instead of push mode to control when clients use network resources to download policies and content updates.
- Increase the heartbeat interval. For fewer than 100 clients per server, increase the heartbeat to 15-30 minutes. For 100 to 1,000 clients, increase the heartbeat to 30-60 minutes. Larger environments might need a longer heartbeat interval. Symantec recommends that you leave **Let clients upload critical events immediately** checked.
- Increase the download randomization to between one and three times the heartbeat interval.

[Randomizing content downloads from the default management server or a Group Update Provider](#)

[Updating policies and content on the client using push mode or pull mode](#)

### **Step 5: Activate the product license**

Purchase and activate a license within 60 days of product installation.

[Licensing Symantec Endpoint Protection](#)

[Symantec Endpoint Protection product license terminology](#)

[Activating or importing your Symantec Endpoint Protection product license](#)

### **Step 6: Decide on a client deployment method**

Determine which client deployment method would work best to install the client software on your computers in your environment.

[Choosing a method to install the client using the Client Deployment Wizard](#)

- For Linux clients, you can use either **Save Package** or **Web Link and Email**, but not **Remote Push**.
- For Windows and Mac clients, if you use **Remote Push**, you may need to do the following tasks:
  - Make sure that administrator access to remote client computers is available. Modify any existing firewall settings (including ports and protocols) to allow remote deployment between Symantec Endpoint Protection Manager and the client computers.  
[Communication ports for Symantec Endpoint Protection](#)
  - You must be logged on with an account that grants local administrator access.  
If the client computers are part of an Active Directory domain, you must be logged on to the computer that hosts Symantec Endpoint Protection Manager with an account that grants local administrator access to the client computers. You should have administrator credentials available for each client computer that is not part of an Active Directory domain.

[Preparing Windows and Mac computers for remote deployment](#)

[Preparing for client installation](#)

### **Step 7: Prepare the client for installation**

1. Make sure that the computers on which you install the client software meet the minimum system requirements. You should also install the client on the computer that hosts Symantec Endpoint Protection Manager.  
See: [Release notes, new fixes, and system requirements for all versions of Endpoint Protection](#)
2. Manually uninstall any third-party security software programs from Windows computers that the Symantec Endpoint Protection client installer cannot uninstall.  
For a list of products that this feature removes, see: [Third-party security software removal support in Symantec Endpoint Protection](#)  
You must uninstall any existing security software from Linux computers or from Mac computers.  
Some programs may have special uninstallation routines, or may need to have a self-protection component disabled. See the documentation for the third-party software.

- 
3. As of 14, you can configure the installation package to remove a Windows Symantec Endpoint Protection client that does not uninstall through standard methods. When that process completes, it then installs Symantec Endpoint Protection.

[Configuring client packages to uninstall existing security software](#)

### Step 8: Deploy and install the client software

1. For Windows clients, do the following tasks:
  - Create a custom client install feature set that determines which components you install on the client computers. You can also use one of the default client install feature sets.  
[Importing existing groups and computers from an Active Directory or an LDAP server](#)  
For client installation packages for workstations, check the email scanner protection option that applies to the mail server in your environment. For example, if you use a Microsoft Exchange mail server, check **Microsoft Outlook Scanner**.
  - Update custom client install settings to determine installation options on the client computer. These options include the target installation folder, the uninstallation of third-party security software, and the restart behavior after installation completes. You can also use the default client install settings.  
[Choosing which security features to install on the client](#)
2. With the Client Deployment Wizard, create a client installation package with selections from the available options, and then deploy it to your client computers. You can only deploy to Mac or Windows computers with the Client Deployment Wizard.
  - [Installing Symantec Endpoint Protection clients with Web Link and Email](#)
  - [Installing Symantec Endpoint Protection clients with Remote Push](#)
  - [Installing Symantec Endpoint Protection clients with Save Package](#)
  - [Exporting client installation packages](#)

Symantec recommends that you do not perform third-party installations simultaneous to the installation of Symantec Endpoint Protection. The installation of any third-party programs that make network- or system-level changes may cause undesirable results when you install Symantec Endpoint Protection. If possible, restart the client computers before you install Symantec Endpoint Protection.

### Step 9: Check that the computers are listed in the groups that you expected and that the clients communicate with the management server

In the management console, on the **Clients > Clients** page:

1. Change the view to **Client status** to make sure that the client computers in each group communicate with the management server.  
**Look at the information in the following columns:**
  - The **Name** column displays a green dot for the clients that are connected to the management server.  
[Checking whether the client is connected to the management server and is protected](#)
  - The **Last Time Status Changed** column displays the time that each client last communicated with the management server.
  - The **Restart Required** column displays whether or not the client computers need to be restarted to be protected.  
[Restarting the client computers from Symantec Endpoint Protection Manager](#)
  - The **Policy Serial Number** column displays the most current policy serial number. The policy might not update for one to two heartbeats. You can manually update the policy on the client if the policy does not update immediately.  
[Using the policy serial number to check client-server communication](#)  
[Updating client policies](#)
2. Change to the **Protection technology** view and ensure that the status is set to **On** in the columns between and including **AntiVirus Status** and **Tamper Protection Status**.  
[Viewing the protection status of client computers](#)

- 
3. On the client, check that the client is connected to a server, and check that the policy serial number is the most current one.

[Checking the connection to the management server on the client computer](#)

[Checking whether the client is connected to the management server and is protected](#)

[Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)

## Symantec Endpoint Protection Quick Start Guide

This guide helps you download, install, and configure Symantec Endpoint Protection, and is designed for default, first-time managed installations of 500 clients or fewer.

To upgrade, see: [Upgrading and Migrating to the Latest Release of Symantec Endpoint Protection \(SEP\)](#)

### Preinstall: Check system requirements

Before you install Symantec Endpoint Protection Manager or the Symantec Endpoint Protection clients, perform the following steps:

1. Download [SymDiag](#) and run the preinstall check to ensure the computer(s) meet system requirements.
2. Review the [release notes and system requirements for Symantec Endpoint Protection](#).

### Step 1: Download the Symantec Endpoint Protection installation file

You download the latest version of Symantec software and tools, retrieve license keys, and activate your product through the [Broadcom Support Portal](#). See:

- [Symantec Getting Started](#) and scroll down to **On-Premises Security Products**.
- [Download the latest version of Symantec software](#)

### Step 2: Install the Symantec Endpoint Protection Manager

If you cannot find or otherwise download your Symantec software through the Broadcom Support Portal, contact [Customer Care](#) for assistance.

1. In the folder where you downloaded the Symantec Endpoint Protection installation file, double-click the file to extract all files. If you see an **Open File - Security Warning** prompt, click **Run**.
2. Do one of the following actions, depending on the version of your installation:
  - **For versions 14.2 MP1a (14.2.1023.0100) or later**, the file extracts to C:\Users\username\AppData\Local\Temp\7zXXXXXXXXXX, where XXXXXXXXXX represents a random string of letters and numbers. Setup.exe automatically launches. Leave the installation menu open until the installation completes. Closing the menu deletes all of the files in the temporary directory.  
To save the installation files, navigate to the previously described temp folder and copy its contents to a location that you select. The installation files include the Tools directory.
  - **For versions earlier than 14.2 MP1a (14.2.1023.0100)**, type or browse to a location to extract to, and then click **Extract**. When the extraction finishes, find and double-click Setup.exe.
3. Click **Install Symantec Endpoint Protection**.
4. Continue with the installation by accepting the terms in the license agreement, along with all default prompts, and then click **Install**.
5. On the **Welcome to the Management Server Configuration Wizard** panel, click **Default configuration**, and then click **Next**.  
For a customized installation, such as using a SQL Server database, click **Custom configuration**.
6. Fill out the required fields to create the system administrator account and email address to which Symantec Endpoint Protection Manager sends notifications, and then click **Next**.

---

You must configure the mail server to receive notification and password reset emails from the management server. You can also enter specified mail server information, and then click **Send Test Email** (optional).

7. Choose the following options, and then click **Next**:
  - Whether or not you want to run LiveUpdate after the installation finishes. Symantec recommends that you run LiveUpdate during installation. (14.3 MPx and earlier)
  - Whether or not Symantec collects data from the clients.
  - Partner information, if it applies to your licensing situation.This step may take some time to finish.
8. On the **Configuration completed** panel, click **Finish** to launch Symantec Endpoint Protection Manager.
9. On the Symantec Endpoint Protection Manager logon screen, type the user name and password you created in step 6 and confirm that you can log on.  
Your user name is `admin` by default.

If you need a SQL Server database for an environment with 500 or fewer clients, see: [Installing Symantec Endpoint Protection Manager with a custom configuration](#)

You have the option to manage Symantec Endpoint Protection clients from the Symantec Endpoint Security cloud console. You would then enroll the Symantec Endpoint Protection Manager domain any time after installation completes. See: [Enrolling a domain in the cloud console from the Symantec Endpoint Protection Manager console](#)

### Step 3: Activate your license and add a group

After you log on to Symantec Endpoint Protection Manager, the **Getting Started** screen appears with multiple links to common tasks. For example, you can activate your license or deploy Symantec Endpoint Protection clients.

To open this screen at any time, click **Help > Getting Started Page** in the top right-hand corner of Symantec Endpoint Protection Manager. For video tours of other common tasks within Symantec Endpoint Protection Manager, click **Take a feature tour**.

#### To activate your product license:

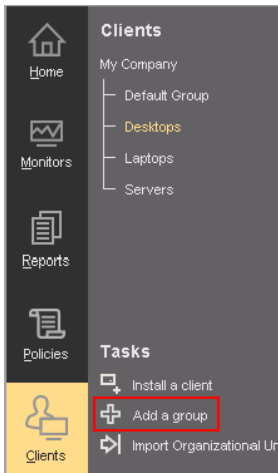
1. In the Symantec Endpoint Protection Manager, in the left pane, click **Admin > Licenses**.
2. Under **Tasks**, click **Activate license**.
3. Using your serial number or the .SLF license file that your order fulfillment email contains, follow the prompts to install your license.

#### To add a group for clients:

Symantec recommends that you create separate groups for desktops, laptops, and servers.

1. In the Symantec Endpoint Protection Manager, in the left pane, click **Clients**.
2. Under **Clients**, click **My Company**.
3. Under **Tasks**, click **Add a group**.
4. In the **Add Group for My Company** dialog box, type the group name and a description, and then click **OK**.

You can then further configure the group settings, such as policy inheritance.



#### Step 4: Install the Symantec Endpoint Protection clients

Before you install the clients by using Symantec Endpoint Protection Manager, check the following items:

- Make sure that the computers can be accessed through the network.
- Make sure that you have administrator credentials for the computers to which you want to deploy.

For unmanaged client installations, see: [Installing an unmanaged Windows client](#)

1. In Symantec Endpoint Protection Manager, in the left pane, click **Clients**.
2. Under **Clients**, select the group you created previously.
3. Under **Tasks**, click **Install a client**.
4. In the **Welcome to the Client Deployment Wizard** panel, click **New Package Deployment**, and then click **Next**.
5. In the **Install Packages** drop-down list, select the operating system that matches the operating system of the client computers.
6. Choose the following options depending on the operating system you selected in the previous step.
  - **Windows install package:**
    - In the **Install Feature Sets** drop-down list, keep the default setting of **Full Protection for Clients**.
    - In the **Install Settings** drop-down list, keep the default setting of **Default Standard client installation settings for Windows**.

These default settings require a restart. To change the restart settings, you need to add a custom Install Settings package first. After you add the client package, click **Options** to select the custom package. See: [Creating custom client installation packages in Symantec Endpoint Protection Manager](#).
    - Choose whether to include virus definitions next to **Content Options**, and then click **Next**.
  - **Mac install package:**

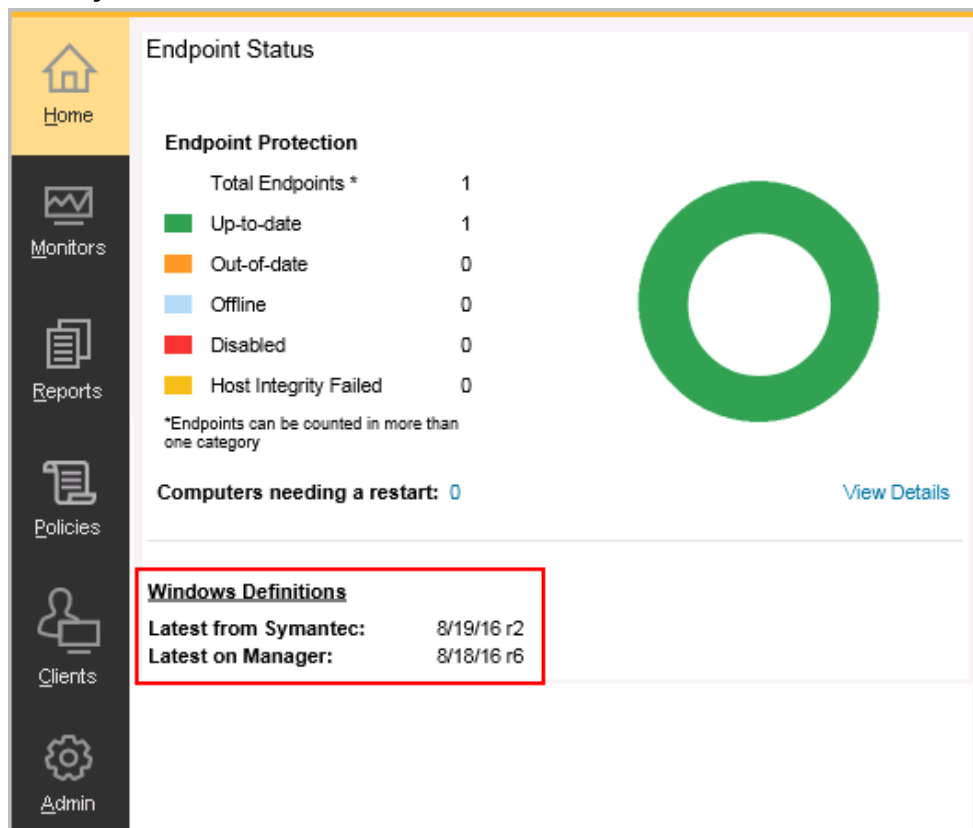
Keep the default setting for **Upgrade settings**, and then click **Next**.
  - **Linux install package:**

Click **Next**. Linux packages are limited to the **Web Link and Email** or **Save Package** deployment method.  
[Installing the Symantec Endpoint Protection for Linux client \(14.3 MP1 and earlier\)](#)  
[Installing the Symantec Agent for Linux 14.3 RU1](#)
7. Click **Remote Push**, and then click **Next**.
8. On the **Browse Network** tab, browse to your workgroup or domain and select the computers you want to push the Symantec Endpoint Protection client to. After you select the computers, click the **>>** option to add them to the right pane.
9. After you add the desired computers, click **Next**.
10. Click **Send** to initiate the process.

- After the push installation has finished, you see a **Deployment Summary** window with the results of the push.
11. Click **Next**, and then click **Finish** to exit the wizard.  
This window indicates that the install files were successfully copied.
  12. To confirm that the client was successfully installed, check that the client exists in the client group that you added in the **Clients** pane.  
[Checking whether the client is connected to the management server and is protected](#)

#### Step 5: Check that the latest definitions are installed

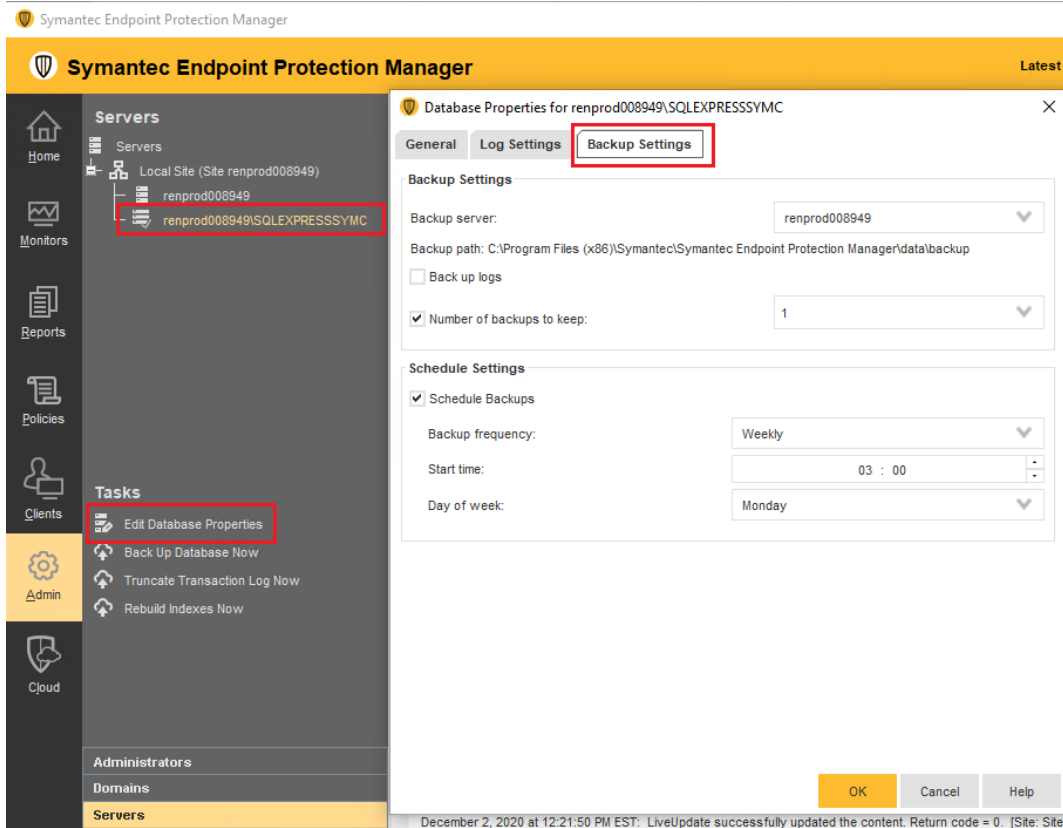
1. In Symantec Endpoint Protection Manager, in the left pane, click **Home**.
2. In the **Endpoint Status** box, under **Windows Definitions**, compare the dates for **Latest on Manager** and **Latest from Symantec**.



3. If the dates do not match, click **Help > Getting Started Page**, click **Run LiveUpdate now**, and then click **Download**.

#### Step 6: Check the database backup settings

1. In Symantec Endpoint Protection Manager, in the left pane, click **Admin > Servers**.
2. Under **Servers**, click **Local Site (My Site) > SQLEXPRESSSYMC**.  
For 14.3 MPx and earlier, click **localhost**.
3. Under **Tasks**, click **Edit Database Properties**.
4. On the **Backup Settings** tab, make any necessary adjustments and then click **OK**.  
By default, a backup is saved once a week.



## Appendix A: Additional resources and guides

[Product guides and manuals for Symantec Endpoint Protection](#)

[Best practices for Symantec Endpoint Protection](#)

[Communication ports that Symantec Endpoint Protection uses](#)

[Error: "...services require user rights" or "...cannot read the user rights" during installation or configuration](#)

## Installing Symantec Endpoint Protection Manager

You perform several tasks to install the management server and the console. In the installation wizard, a green check mark appears next to each completed task.

For the most current system requirements, see: [Release notes, new fixes, and system requirements for all versions of Endpoint Protection](#)

Some Symantec products may cause conflicts with Symantec Endpoint Protection Manager when they are installed on the same server. For information about any necessary configuration changes in those products, see: [Software compatibility with Symantec Endpoint Protection](#)

In addition, Symantec Endpoint Protection Manager installation and configuration checks the security policies for the required rights to allow the virtual service accounts to run correctly. Symantec Endpoint Protection Manager automatically changes local security policies, and alerts you to changes you need to make to domain security policies. You can also change your security policies before installation. See [How to assign user rights to the Windows Security Policies for Symantec Endpoint Protection Manager services](#).

---

## NOTE

Symantec Endpoint Protection Manager requires full access to the system registry for installation and normal operation. To prepare a Windows Server 2003 computer on which you plan to remotely install Symantec Endpoint Protection Manager, you must first allow remote control on the computer. When you connect with Remote Desktop, you must also use a console session or shadow the console session in Remote Desktop.

## NOTE

If you install Symantec Endpoint Protection Manager 14.2 in an IPv6 network, you must also have the IPv4 stack available for Java, even if IPv4 is disabled. If the IPv4 stack is uninstalled, Java does not work, and the Symantec Endpoint Protection Manager installation fails.

### To install Symantec Endpoint Protection Manager:

1. If you downloaded the product, extract the entire installation file to a physical disk, such as a hard disk. Run **Setup.exe** from the physical disk.

The installation should start automatically. If it does not start, open the installation file, and then double-click **Setup.exe**.

2. In the **Symantec Endpoint Protection Installation Program** dialog box, click **Install Symantec Endpoint Protection**, and then click **Install Symantec Endpoint Protection Manager**.
3. Review the sequence of installation events, and then click **Next** to begin.
4. In the **License Agreement** panel, click **I accept the terms in the license agreement**, and then click **Next**.
5. In the **Destination Folder** panel, accept the default destination folder or specify another destination folder, and then click **Next**.
6. Click **Install**.

The installation process begins for the Symantec Endpoint Protection Manager management server and console. When the installation is complete, click **Next**.

7. After the initial installation completes, you configure the server and database. Click **Next**.

The **Management Server Configuration Wizard** starts.

[Configuring Symantec Endpoint Protection Manager after installation](#)

[Installing Symantec Endpoint Protection Manager with a custom configuration](#)

[Getting up and running on Symantec Endpoint Protection Manager for the first time](#)

## Configuring Symantec Endpoint Protection Manager after installation

The Management Server Configuration Wizard automatically starts after the Symantec Endpoint Protection Manager installation. You configure the management server according to your requirements.

You can also start the Management Server Configuration Wizard at any time after installation from **Start > All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Tools**.

1. [Installing Symantec Endpoint Protection Manager](#)

2. With the **Default configuration for new installation** selected, click **Next**.

The default configuration automatically installs the default database, Microsoft SQL Server Express (as of 14.3 RU1). Version 14.3 MPx and earlier installs the embedded database as the default database.

3. Enter company name, a password for the default administrator `admin`, and an email address.

Alternately, you can add details to use a specified mail server.



- 
4. Optionally click **Send Test Email**.

Symantec Endpoint Protection Manager sends password recovery information and other important notifications to this email account, so you should not proceed with configuration if you do not receive the email.

5. Once you verify that you receive the test email, click **Next**.

For 14.3 MPx and earlier, indicate whether you want to run LiveUpdate as part of the installation. Click **Next**. As of 14.3 RU1, LiveUpdate runs automatically as part of a new installation.

6. You can also add the optional **Partner Information**, if a partner manages your Symantec licenses, and then click **Next**.

7. Indicate whether you want Symantec to receive pseudonymous data, and then click **Next** to begin the database creation.

The database creation can take several minutes.

8. When the database creation completes, click **Finish** to complete the Symantec Endpoint Protection Manager configuration.

The Symantec Endpoint Protection Manager console logon screen appears if you leave the option checked to launch Symantec Endpoint Protection Manager. Once you log on, you can begin client deployment.

[Logging on to the Symantec Endpoint Protection Manager console](#)

You can find a configuration summary in the following location on the server where Symantec Endpoint Protection Manager is installed:

ProgramFiles\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\SEPMConfigurationSummaryInfo.txt

## Installing Symantec Endpoint Protection Manager with a custom configuration

When you want to install Symantec Endpoint Protection Manager with a Microsoft SQL Server database or want to install multiple sites, you should choose **Custom configuration** in the **Management Server Configuration Wizard**. When you select this option, additional settings become available.

### NOTE

To provide connectivity to the database, you must install SQL Server client tools on the server that runs Symantec Endpoint Protection Manager.

[About SQL Server configuration settings](#)

**To install Symantec Endpoint Protection Manager with a custom configuration:**

1. [Installing Symantec Endpoint Protection Manager](#)
2. In the **Management Server Configuration Wizard**, click **Custom configuration for new installation**, and then click **Next**.

If you have fewer than 500 computers, Symantec recommends that you click **Default configuration for new installation**.

[Configuring Symantec Endpoint Protection Manager after installation](#)

3. Click **Install my first site**, and then click **Next**.

The following options are for advanced installations and do not apply to first-time installations of Symantec Endpoint Protection Manager:

- 
- For **Install an additional management server to an existing site**, see: [Setting up failover and load balancing](#)
  - For **Install an additional site**, see:
    - [Setting up sites and replication](#)
    - [How to install a second site for replication](#)
    - [How replication works](#)
4. On this screen, you can customize the following settings, and then click **Next**:
    - Site name
    - Server name
    - Port numbers

You should contact your network administrator before you make changes to the default Symantec Endpoint Protection Manager port configurations.
    - The location of the Symantec Endpoint Protection Manager server data folder

If there is not enough available free space on the drive on which Symantec Endpoint Protection Manager is installed, relocate the server data folder to an alternate drive.
  5. On the database selection screen, click **Microsoft SQL Server database** and then click **Next**.
    - If you select the **Default Microsoft SQL Server Express database** for a custom configuration for 5,000 clients or less, go to step 9. However, the rest of this procedure assumes that you select the Microsoft SQL Server database.
    - Check with your SQL database administrator to confirm whether or not the automatic database maintenance tasks should be enabled.
    - Symantec recommends that you host the SQL Server and Symantec Endpoint Protection Manager on separate physical servers.
    - For information on supported versions of Microsoft SQL Server, see the [system requirements for Symantec Endpoint Protection](#).
  6. Click **Create a new database**, and then click **Next**.

**NOTE**

Using an existing database is considered an advanced installation option, and typically does not apply to new installations.
  7. On the **Step One: Database Server Authentication** screen, fill in the details for the SQL Server to which Symantec Endpoint Protection Manager connects, and then click **Connect to database**.

If the database connection is successful, the **Step Two: New Database Creation** section becomes available.
  8. Under **Step Two: New Database Creation**, fill in the details to create a new database, and then click **Next**.

For questions regarding either **Database Server Authentication** or **Database Creation**, contact your SQL Server database administrator.
  9. Enter company name, a password for the default administrator admin, and an email address.

Alternately, you can add details to use a specified mail server.
  10. Click **Send Test Email**. Once you verify that you receive the test email, click **Next**.

Symantec Endpoint Protection Manager sends password recovery information and other important notifications to this email account, so you should not proceed with configuration if you do not receive the email.
  11. Create an encryption password, or choose to use a random password, and then click **Next**.

This password is used to protect the communication between clients and Symantec Endpoint Protection Manager, and is stored in the Symantec Endpoint Protection Manager recovery file.
-

- 
12. Indicate whether you want to run LiveUpdate as part of the installation. If you run LiveUpdate as part of a new installation, content is more readily available for the clients you deploy. Click **Next**

You can also add the optional **Partner Information**, if a partner manages your Symantec licenses.

13. Indicate whether you want Symantec to receive pseudonymous data, and then click **Next** to begin the database creation.

14. After the database is created and initialized (which may take several minutes), click **Finish**.

The Symantec Endpoint Protection Manager console logon screen appears if you leave the option checked to launch Symantec Endpoint Protection Manager. Once you log on, you can begin client deployment.

[Logging on to the Symantec Endpoint Protection Manager console](#)

You can find a configuration summary in the following location on the server where Symantec Endpoint Protection Manager is installed:

ProgramFiles\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\SEPMConfigurationSummaryInfo.txt

[About choosing a database type](#)

## Logging on to the Symantec Endpoint Protection Manager console

You log on to the Symantec Endpoint Protection Manager console after you install Symantec Endpoint Protection Manager. You can log on to the console in either of two ways:

1. Locally, from the computer on which you installed the management server.  
You can also access the reporting functions from a standalone web browser that is connected to your management server.  
[Logging on to reporting from a standalone web browser](#)
2. Remotely, from any computer that meets the system requirements for a remote console and has network connectivity to the management server. You can log on to the remote web console or the remote Java console.

[Logging on Symantec Endpoint Protection Manager remotely](#)

For security, the console logs you out after a maximum of one hour. You can decrease this period of time.

[Changing the timeout period for staying logged on to the Symantec Endpoint Protection Manager console](#)

### Logging on to the console locally

To log on to the console locally:

1. Go to **Start > Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager**.
2. In the **Symantec Endpoint Protection Manager** logon dialog box, type the user name (`admin` by default) and the password that you configured during the installation.

Optionally check **Remember my user name**, **Remember my password** or both, if available.

[Displaying the Forgot your password? link so that administrators can reset lost passwords](#)

- To log on using a PIV card or CAC, click **Options**, and then check **Log on to a smart card** (14.2 or later). In the **Login / PIN** message, type your pin number.

[Configuring Symantec Endpoint Protection Manager to authenticate administrators who log on with smart cards](#)

- To log on using two-factor authentication, type the password immediately followed by the token. If you omit the token, the logon attempt fails. If you use the Symantec VIP smartphone app, type the password, and then approve the request on the app after you click **Log On**. If you do not approve the request within two minutes, the logon attempt fails.

[Configuring two-factor authentication with Symantec VIP](#)

If the console has more than one domain, click **Options** and type the domain name. [Adding a domain](#)

3. Click **Log On**.

---

## Logging on to the console remotely

To log on remotely, you need to know the IP address or the host name of the computer on which the management server is installed. Also, make sure that your web browser Internet options let you view content from the server you log on to and that the web browser is supported. For a list of supported web browsers, see:

[Release notes, new fixes, and system requirements for all versions of Endpoint Protection](#)

### To find the IP address or host name:

1. Log on locally.
2. On the **Home** page under **Favorite Reports**, click **Risk Distribution by Protection Technology**.
3. At the bottom of the **Risk Distribution by Protection Technology** dialog box, look for the text: You can launch the Symantec Endpoint Protection Manager using: `http://SEPMServer:9090/symantec.html`.

#### NOTE

To install the remote console if you haven't already, click `http://SEPMServer:9090/symantec.html` and follow the instructions.

When you log on remotely, you can perform the same tasks as administrators who log on locally. What you can view and do from the console depends on the type of administrator you are. Most administrators in smaller organizations log on as a system administrator. On Microsoft Windows Server 2008 and Windows 7, you must have administrative privileges on the computer where you access the remote console and you must run it using administrative privileges. You can configure the console icon or **Start** menu item to launch using your administrative privileges.

### To launch the remote console with administrator privileges:

1. Right-click the **Symantec Endpoint Protection Manager Console** icon on the Windows desktop or the **Symantec Endpoint Protection Manager Console** entry on the **Start** menu.
2. Click **Properties > Advanced > Run as Administrator** or **More > Run as administrator**.

For Windows Server 2016, use the host name of the computer on which the management server is installed.

#### NOTE

If you installed the remote Java console with an earlier version of the product, you must reinstall it when you upgrade to a later version. Starting in 14.3, you cannot log on to the Symantec Endpoint Protection Manager thick remote console if you run a 32-bit version of Windows. The Oracle Java SE Runtime Environment no longer supports 32-bit versions of Microsoft Windows. As of 14.3, the remote web console uses JRE version 11.

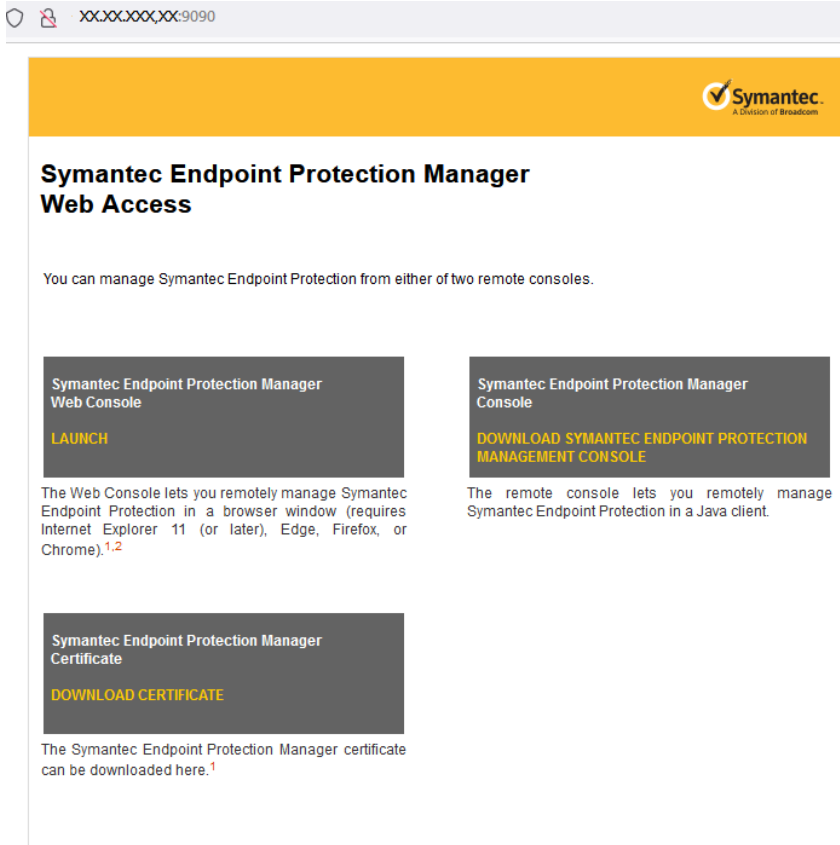
### To log on to the console remotely:

1. Open a supported web browser and type the following address in the address box:

`http://SEPMServer:9090/`

Where SEPMServer is the host name or IP address of the management server.

IP addresses include IPv4 and IPv6 (14.2 and later). You must enclose the IPv6 address with square brackets. For example: `http://[SEPMServer]:9090/`



2. On the Symantec Endpoint Protection Manager console Web Access page, click the desired console type.
  - If you click **Symantec Endpoint Protection Manager Web Console**, a secure webpage loads so you log on remotely without the use of the Java Runtime Environment (JRE).
  - If you click **Symantec Endpoint Protection Manager Console**, the computer from which you log on must have the JRE installed to run the Java client. If it does not, you must download and install it. Follow the prompts to install the JRE, and follow any other instructions provided.

The other option is not a remote management solution. You can click **Symantec Endpoint Protection Manager Certificate** to prompt you to download the management console's certificate file. You can then import this file into your web browser if needed.
3. If a host name message appears, click **Yes**.
 

This message means that the remote console URL that you specified does not match the Symantec Endpoint Protection Manager certificate name. This problem occurs if you log on and specify an IP address rather than the computer name of the management server.

If the webpage security certificate warning appears, click **Continue to this website (not recommended)** and add the self-signed certificate.
4. Follow the prompts to complete the logon process.
 

When you log on for the first time after installation, use the account name `admin`.

Depending on the logon method, you may need to provide additional information. For instance, if the console has multiple domains, click **Options** and provide the name of the domain to which you want to log on.
5. If you use the Java-based console, you may have the option to save the user name and password. Click **Log On**.
 

You may receive one or more security warning messages as the remote console starts up. If you do, click **Yes**, **Run**, **Start**, or their equivalent, and continue until the console appears.

You may need to accept the self-signed certificate that the Symantec Endpoint Protection Manager console requires. [About accepting the self-signed server certificate for Symantec Endpoint Protection Manager](#)

---

[Granting or blocking access to remote Symantec Endpoint Protection Manager consoles](#)

[Displaying a message for administrators to see before logging on to the Symantec Endpoint Protection Manager console](#)

## Activating or importing your Symantec Endpoint Protection product license

You can use the License Activation Wizard workflow to perform the following tasks:

- Activating a new paid license.
- Converting a trial license to a paid license.
- Renewing a license.
- Activate an additional paid license in response to an over-deployment status.

You can import and activate a license with a file or serial number that you received from your preferred reseller. See [Partner Locator](#)

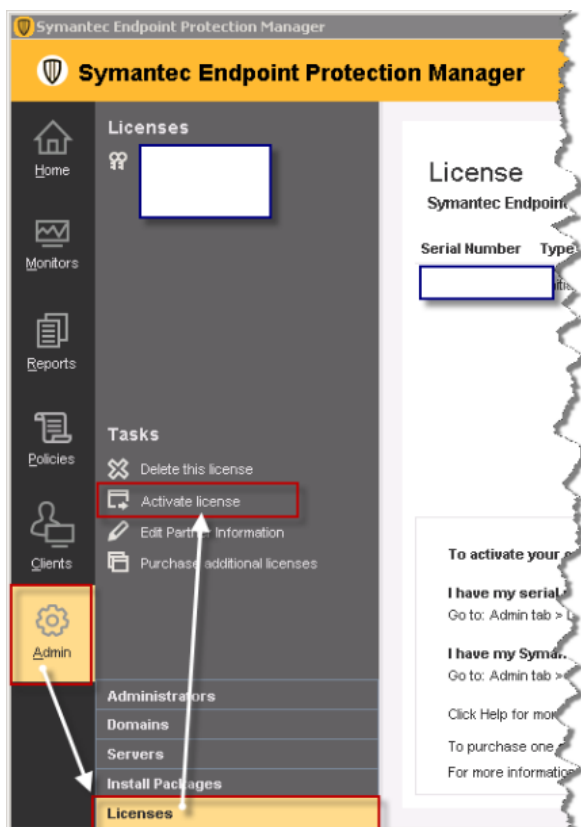
You can start the License Activation Wizard in the following ways:

- The Getting Started screen that appears after you install the product.  
You can also access the Getting Started screen through **Help > Getting Started Page**.
- The **Admin** page of the Symantec Endpoint Protection Manager console.

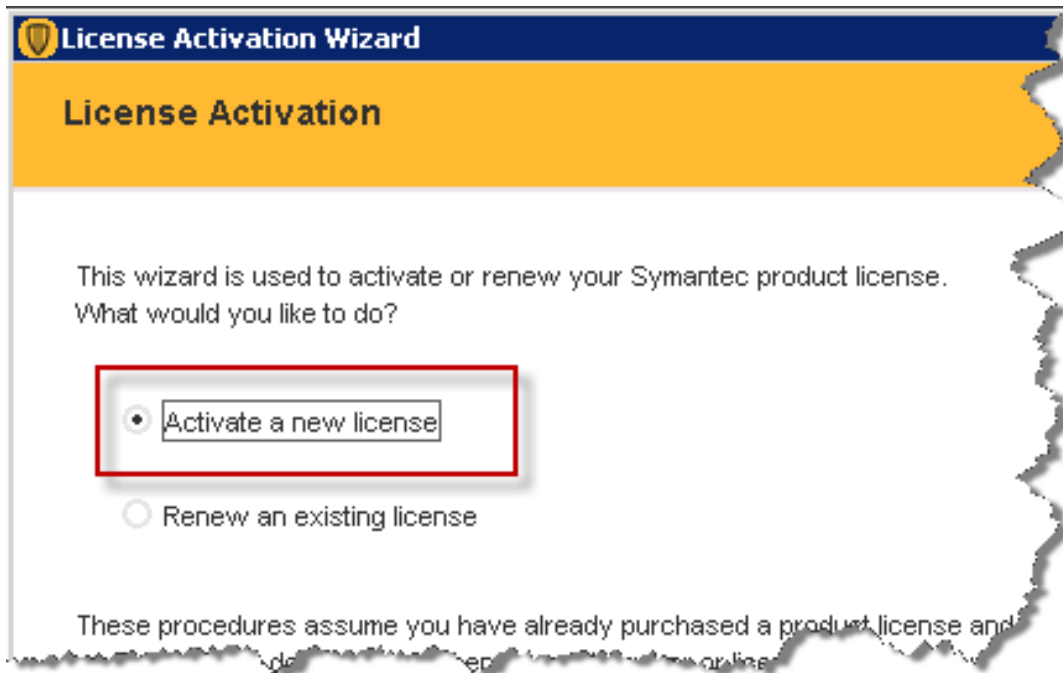
If you activate or import your license from the Getting Started screen, you can skip to step 3.

**To activate or import your Symantec Endpoint Protection product license:**

1. In Symantec Endpoint Protection Manager, click **Admin > Licenses**.
2. Under **Tasks**, click **Activate license**.



3. Click **Activate a new license**, and then click **Next**. If you do not see this panel, continue to the next step.



**License Activation Wizard**

## License Activation

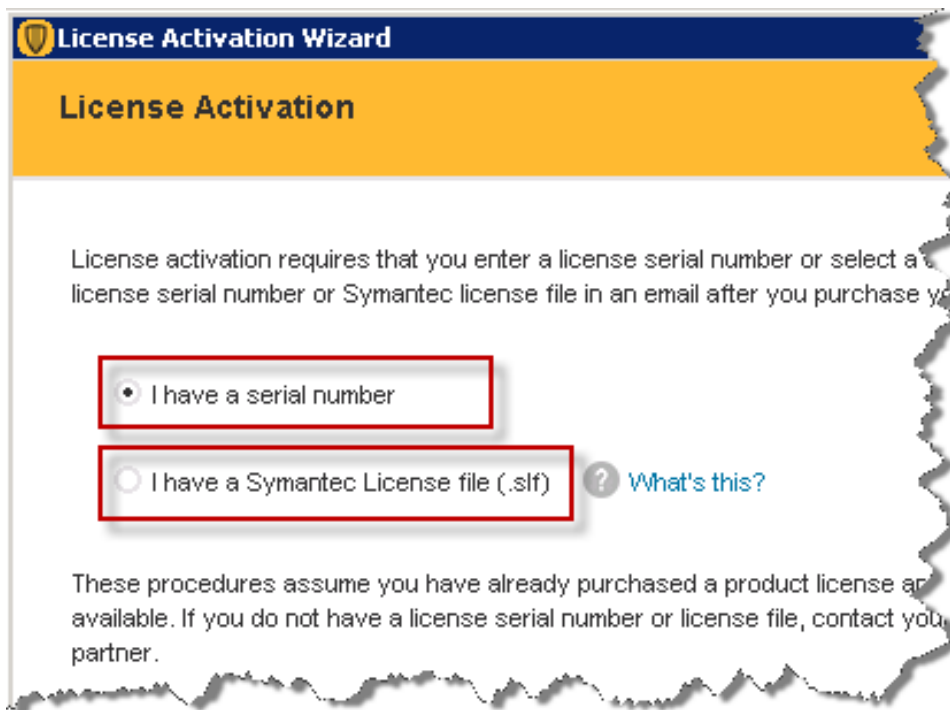
This wizard is used to activate or renew your Symantec product license.  
What would you like to do?

☒ **Activate a new license**

☐ Renew an existing license

These procedures assume you have already purchased a product license and

4. On the **License Activation** panel, select the option that matches your situation, and then click **Next**.



**License Activation Wizard**

## License Activation

License activation requires that you enter a license serial number or select a  
license serial number or Symantec license file in an email after you purchase yo

☒ **I have a serial number**

☐ I have a Symantec License file (.slf) [? What's this?](#)

These procedures assume you have already purchased a product license and  
available. If you do not have a license serial number or license file, contact you  
partner.

The following table describes each option:

Option	Description
<b>I have a serial number</b>	You may receive a license serial number when you or your preferred reseller purchased the license. If you have a license serial number, select this option. If you have a serial number, select <b>I have a Symantec License File</b> .
<b>I have a Symantec License File (.slf)</b>	In most cases, you receive a Symantec license file (.slf file) in an email from Broadcom shortly after you complete the purchase process. The file arrives attached to the notification email as a .zip file. If you have received a .slf file, select this option. <b>Note:</b> You must extract the .slf file from the .zip file before you can use it to activate your product license. <b>Warning!</b> The .slf file contains the information that is unique to your license. To avoid corrupting the license file, do not alter its contents. You may copy the file for your records.

5. Do one of the following tasks based on the selection that you made in the previous step:

- If you selected **I have a serial number**, enter the serial number, and then click **Submit**. Review the information about the license you added, and then click **Next**.

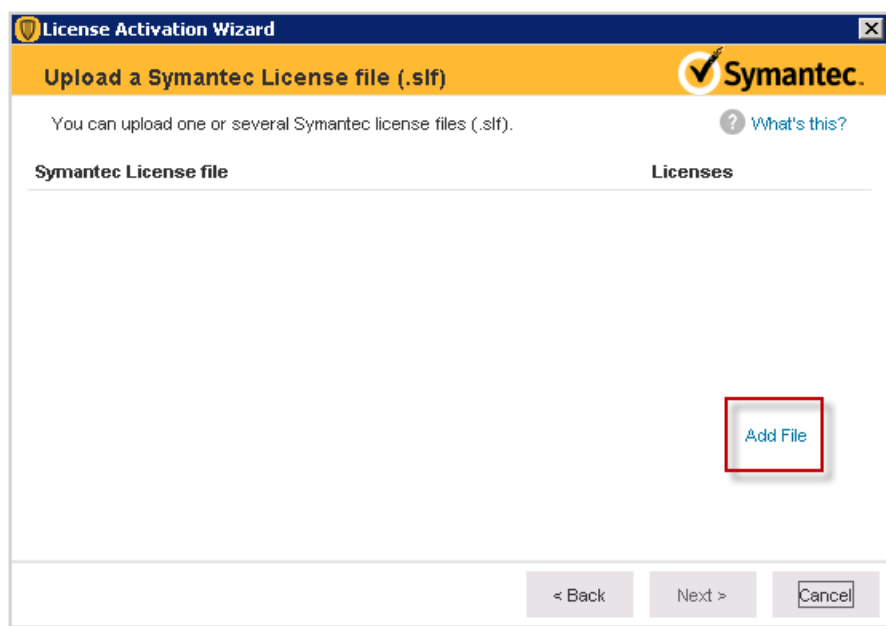
**NOTE**

To activate a license with a serial number, you must have an active internet connection and be able to reach the Symantec Licensing Server. If the connection succeeds, the Symantec home page loads.



- If you selected **I have a Symantec License File (.slf)**, click **Add File**. Browse to and select the .slf file you extracted from the .zip file that came with your Symantec notification email. Click **Open**, and then click **Next**.





6. Enter information about your technical contacts and primary contacts, and about your company. Click to acknowledge the disclosure statement, and then click **Submit**.  
If you provided this information when you purchased your license, this panel does not display.
7. Click **Finish**.

[Purchasing Symantec Endpoint Protection licenses](#)

[Licensing Symantec Endpoint Protection](#)

## Purchasing Symantec Endpoint Protection licenses

**You need to purchase a license in the following situations:**

- Your trial license expired. Symantec Endpoint Protection comes with a trial license that lets you install and evaluate the product in your environment.
- Your current license is expired.
- Your current license is over-deployed. Over-deployed means that you have deployed more clients than your current license allows.

Depending upon how you purchase your license, you receive by email either a product license serial number or a Symantec License file. The license file uses the file extension .slf. When you receive the license file by email, it is attached to the email as a .zip file. You must extract the .slf file from the .zip file.

**To purchase or renew a license:**

- Contact your [preferred reseller](#).

Save the license file to a computer that can be accessed from the Symantec Endpoint Protection Manager console. Many users save the license on the computer that hosts Symantec Endpoint Protection Manager. Many users also save a copy of the license to a different computer or removable storage media for safekeeping.

### **WARNING**

To prevent corruption of the license file, do not open or alter the file contents in any way. However, you may copy and store the license as desired.

[Symantec Endpoint Protection product license requirements](#)

## Installing Symantec Endpoint Protection clients with Save Package

If you have a small number of clients, use the Save Package method to deploy and install the installation package on the clients.

Save Package creates the installation packages that you can install manually, with third-party deployment software, or with a login script.

Save Package comprises the following tasks:

- You make your configuration selections and then create the client installation packages.
- You save the installation package to a folder on the computer that runs Symantec Endpoint Protection Manager. For Windows, the installation package can be for 32- or 64-bit operating systems. The installation package comprises one setup.exe file or a collection of files that includes a setup.exe file. Computer users often find one setup.exe file easier to use.

### NOTE

The Mac and Linux client install packages automatically export a .zip archive file format. To correctly preserve the file permissions, you should expand the archive file with a native archive program, such as the Mac Archive Utility or the ditto command. You cannot use the Mac unzip command, a third-party application, or any Windows application to expand the files for these operating systems

To install Symantec Endpoint Protection clients with Save Package

1. In the console, launch the **Client Deployment Wizard**.

Click **Help > Getting Started Page** and then under **Required tasks**, click **Install the client software on your computers**.

2. In the **Client Deployment Wizard**, do one of the following tasks:
  - Click **New Package Deployment**, and then click **Next**. Save Package only installs a new installation package.
  - Click **Communication Update Package Deployment** if you want to update Windows or Mac client communication settings on the computers that already have the Symantec Endpoint Protection client installed. Follow the on-screen instructions, and then go to step 4.
3. Make selections from the available options, which vary depending on the installation package type, and then click **Next**.

### NOTE

To uninstall existing security software on the Windows client, you must configure custom Client Install Settings before launching the Client Deployment Wizard.

[Configuring client packages to uninstall existing security software](#)

[About the Windows client installation settings](#)

4. Click **Save Package**, and then click **Next**.
5. Click **Browse** and specify the folder to receive the package.

For Communication Update Package Deployment, or for Mac and Linux packages, go to step [Click Next](#).

For new Windows packages, check **Single .exe file (default)** or **Separate files (required for .MSI)**.

### NOTE

Use **Single .exe file** unless you require separate files for a third-party deployment program.

- 
6. Click **Next**.
  7. Review the settings summary, click **Next**, and then click **Finish**.
  8. Provide the exported package to the computer users.

Provide the exported package to the users in the following ways: email, save the package to a secure shared network location, or use a third-party program.

9. Confirm that the user downloads and installs the client software, and confirm the installation status of the clients.

For new Symantec Endpoint Protection installations, the client computers may not appear within Symantec Endpoint Protection Manager until after they restart, either automatically or by action you or the user takes. Mac clients automatically prompt a restart when installation completes. Linux clients do not require a restart.

[Restarting the client computers from Symantec Endpoint Protection Manager](#)

[Running a report on the deployment status of clients](#)

[Choosing which security features to install on the client](#)

[Choosing a method to install the client using the Client Deployment Wizard](#)

[Preparing for client installation](#)

## Installing the Symantec Endpoint Protection client for Mac

You can directly install a Symantec Endpoint Protection client on a Mac computer if you cannot use or do not want to use Remote Push. The steps are similar whether the client is unmanaged or managed.

The only way to install a managed client is with a package that Symantec Endpoint Protection Manager creates. You can convert an unmanaged client to a managed client at any time by importing client-server communication settings into the Mac client.

### NOTE

To prepare the Symantec Endpoint Protection client for Mac for use with third-party remote deployment software, see [Exporting and Deploying a Symantec Endpoint Protection client via Apple Remote Desktop or Casper](#).

**Table 18: Methods for installing the Mac client**

If you downloaded the installation file.	<ol style="list-style-type: none"><li>1. Extract the contents to a folder on a Mac computer, and then open the folder.</li><li>2. Open SEP_MAC.</li><li>3. Copy Symantec Endpoint Protection.dmg to the desktop of the Mac computer.</li><li>4. Double-click Symantec Endpoint Protection.dmg to mount the file as a virtual disk. You then install the Symantec Endpoint Protection client for Mac</li></ol>
If you have a client installation package .zip from the <a href="#">Broadcom Support Portal</a> .	<ol style="list-style-type: none"><li>1. Copy the file to the desktop of the Mac computer. The file may be named Symantec Endpoint Protection.zip or Symantec_Endpoint_Protection_version_Mac_Client.zip, where version is the product version.</li><li>2. Right-click <b>Open With &gt; Archive Utility</b> to extract the file's contents.</li><li>3. Open the resulting folder. You then install the Symantec Endpoint Protection client for Mac.</li></ol>

The resulting virtual disk image or folder contains the application installer and a folder called Additional Resources. Both items must be present in the same location for a successful installation. If you copy the installer to another location, you must also copy Additional Resources.

---

## To install the Symantec Endpoint Protection client for Mac:

1. Double-click `Install Symantec Endpoint Protection`.
2. To begin the installation, click **Install**.
3. To install a helper tool that is needed for installing the Symantec Endpoint Protection client, enter your Mac's administrative username and password, and then click **Install Helper**.
4. After the installation, click **Continue** to finish setting up your Symantec Endpoint Protection client.
5. To set up your Symantec Endpoint Protection client, take the following steps:

Authorize the Symantec Endpoint Protection system extension.	In the <b>Security &amp; Privacy</b> dialog box, on the <b>General</b> tab, at <b>System software from application "Symantec Endpoint Protection" was blocked from loading</b> , click <b>Allow</b> . If needed, click the lock icon to make the changes. You must authorize the system extension for Symantec Endpoint Protection to fully function. <a href="#">About authorizing system extensions for Symantec Endpoint Protection for macOS 10.15 or later</a>
Allow full disk access.	In the <b>Security &amp; Privacy</b> dialog box, on the <b>Privacy</b> tab, make sure <b>Symantec System Extension</b> is allowed to access data and administrative settings for all users on your Mac device. If needed, click the lock icon to make the changes.
Allow changes to network profile.	When prompted <b>Symantec Endpoint Protection would like to filter network content</b> , click <b>Allow</b> .

6. Click **Complete**.

## About authorizing system extensions for Symantec Endpoint Protection for macOS 10.15 or later

Requiring the authorization of system extensions is a security feature of macOS 10.15. You must authorize the system extension for Symantec Endpoint Protection to fully function.

To authorize the system extension for Symantec Endpoint Protection, during the setup of your Symantec Endpoint Protection client, in the **Security & Privacy** dialog box, on the **General** tab, at **System software from application "Symantec Endpoint Protection" was blocked from loading**, click **Allow**.

[Installing the Symantec Endpoint Protection client for Mac](#)

## Managing kernel extension authorization when deploying the Symantec Endpoint Protection client for Mac

If you mass-deploy the Symantec Endpoint Protection client for Mac, you may need to take additional steps to ensure that the kernel extensions are authorized. This requirement applies as of macOS 10.13 (High Sierra). The operating system dictates that the authorization must be made at the local computer. You cannot authorize the kernel extension through remote access, nor can you save the kernel authorization through a preconfigured disk image.

To ensure that kernel extensions are properly authorized on Macs, do one of the following:

- Instruct the Mac users to approve the required extension. Any user can approve a kernel extension through the Security & Privacy preference pane, even if they do not have administrator privileges.

---

### [About authorizing kernel extensions for Symantec Endpoint Protection for macOS 10.13 or later](#)

- Enroll your Macs in a mobile device management (MDM) solution. Even if you do not actively manage Macs with this solution, kernel extension authorization reverts to the way it was enforced before macOS 10.13.
- As of macOS 10.13.2, authorize the kernel extensions through mobile device management (MDM) with the use of a team identifier. To authorize the kernel extensions for Symantec Endpoint Protection on macOS, use the team identifier 9PTGMPNXZ2. Consult the documentation for your MDM suite for guidance on how to use this team identifier.

#### **NOTE**

Starting from Symantec Endpoint Protection client for Mac 14.3, the team identifier is Y2CCP3S9W7 and the system extension name is `com.broadcom.mes.systemextension`

- If you use **NetBoot**, **NetInstall**, or **NetRestore**, use the following command while preparing disk images for deployment:

```
spctl kext-consent add 9PTGMPNXZ2
```

This command uses the Symantec team identifier to pre-approve Symantec kernel extensions on Mac.

Team identifiers that are set through this command are stored in non-volatile random-access memory (NVRAM), which persists even when the Mac powers off. If you reset the NVRAM, the kernel extensions require reapproval. If the user also approved the kernel extension through the Security & Privacy pane, then reapproval is not needed.

For more information on kernel extension loading, see the following Apple documentation:

[Prepare for changes to kernel extensions in macOS High Sierra](#)

## **Installing the Symantec Agent for Linux or the Symantec Endpoint Protection client for Linux**

(For 14.3 RU1 and later)

You install Symantec Agent for Linux directly on a Linux device. You cannot deploy the Linux agent from Symantec Endpoint Protection Manager remotely.

To install Symantec Agent for Linux, create an installation package in Symantec Endpoint Protection Manager, transfer the installation package to a Linux device and then run the installer. The installer will configure the new agent and register it with Symantec Endpoint Protection Manager.

#### **NOTE**

Symantec Agent for Linux 14.3 RU1 and later cannot run as an unmanaged client. All management tasks must be performed in Symantec Endpoint Protection Manager or in cloud console.

#### **(For 14.3 RU1 and later) To install the Symantec Management Agent for Linux:**

1. In Symantec Endpoint Protection Manager, create and download the installation package.
2. Move the `LinuxInstaller` package to a Linux device.
3. Make the `LinuxInstaller` file executable:

```
chmod u+x LinuxInstaller
```

4. Run the installer:

```
./LinuxInstaller
```

You must run the command as root.

To view the list of installation options, run `./LinuxInstaller -h`.

5. To verify the installation, navigate to `/usr/lib/symantec` and run `./status.sh` to confirm that the modules are loaded and daemons are running:

```
./status.sh
```

```
Symantec Agent for Linux Version: 14.3.450.1000
```

```
Checking Symantec Agent for Linux (SEPM) status..
```

```
Daemon status:
```

---

```
cafagent          running
sisamdagent       running
sisidsagent       running
sisipsagent       running
Module status:
sisevt            loaded
sisap             loaded
```

Note that `communication status` is only available for cloud-managed clients.

(For 14.3 MP1 and earlier)

You install an unmanaged or managed Symantec Endpoint Protection client directly on a Linux computer. You cannot deploy the Linux client from Symantec Endpoint Protection Manager remotely. The installation steps are similar whether the client is unmanaged or managed.

The only way to install a managed client is with an installation package that you create in Symantec Endpoint Protection Manager. You can convert an unmanaged client to a managed client at any time by importing client-server communication settings into the Linux client.

If the Linux operating system kernel is incompatible with the pre-compiled Auto-Protect kernel module, the installer tries to compile a compatible Auto-Protect kernel module. The auto-compile process automatically launches if it is needed. However, the installer might be unable to compile a compatible Auto-Protect kernel module. In this case, Auto-Protect installs but is disabled. For more information, see:

[Supported Linux kernels for Symantec Endpoint Protection](#)

#### NOTE

You must have superuser privileges to install the Symantec Endpoint Protection client on the Linux computer. The procedure uses `sudo` to demonstrate this elevation of privilege.

**(For 14.3 MP1 and earlier) To install the Symantec Endpoint Protection client for Linux:**

1. Copy the installation package that you created to the Linux computer. The package is a .zip file.
2. On the Linux computer, open a terminal application window.
3. Navigate to the installation directory with the following command:

```
cd /directory/
```

Where `directory` is the name of the directory into which you copied the .zip file.

4. Extract the contents of the .zip file into a directory named `tmp` with the following command:

```
unzip "InstallPackage" -d sepfiles
```

Where `InstallPackage` is the full name of the .zip file, and `sepfiles` represents a destination folder into which the extraction process places the installation files.

If the destination folder does not exist, the extraction process creates it.

5. Navigate to `sepfiles` with the following command:

```
cd sepfiles
```

6. To correctly set the execute file permissions on `install.sh`, use the following command:

```
chmod u+x install.sh
```

7. Use the built-in script to install Symantec Endpoint Protection with the following command:

```
sudo ./install.sh -i
```

Enter your password if prompted.

---

This script initiates the installation of the Symantec Endpoint Protection components. The default installation directory is as follows:

```
/opt/Symantec/symantec_antivirus
```

The default work directory for LiveUpdate is as follows:

```
/opt/Symantec/LiveUpdate/tmp
```

The installation completes when the command prompt returns. You do not have to restart the computer to complete the installation.

(For 14.3 MP1 and earlier) To verify the client installation, click or right-click the Symantec Endpoint Protection yellow shield and then click **Open Symantec Endpoint Protection**. The location of the yellow shield varies by Linux version. The client user interface displays information about program version, virus definitions, server connection status, and management.

[About auto-compile for the Symantec Endpoint Protection client for Linux](#)

[About the Linux client graphical user interface](#)

[Importing client-server communication settings into the Linux client](#)

[Preparing for client installation](#)

[Install Symantec Endpoint Protection 14.x for Redhat based distributions](#)

## Getting started on the Linux agent

The Symantec Endpoint Protection Manager administrator may have enabled you to configure the settings on the Linux agent.

**Table 19: Steps to get started on the Linux agent (for 14.3 RU1 and later)**

Step	Task	Description
Step 1	Install the Symantec Agent for Linux.	The administrator provides you with the installation package for a managed client or sends you a link by email to download it. <a href="#">Installing the Symantec Agent for Linux or the Symantec Endpoint Protection client for Linux</a>
Step 2	Check that the Linux agent communicates with the Symantec Endpoint Protection Manager or cloud console.	To confirm the connection to Symantec Endpoint Protection Manager or cloud console, you can run the following command: <code>/usr/lib/symantec/status.sh</code>
Step 3	Verify that the Auto-Protect is running.	To check the status of Auto-Protect, run the following command: <code>cat /proc/sisap/status</code>
Step 4	Check that the definitions are up to date.	LiveUpdate definitions are available at the following location: <code>/opt/Symantec/sdcssagent/AMD/sef/definitions/</code>

**Table 20: Steps to get started on the Linux client (for 14.3 MP1 and earlier)**

Step	Task	Description
Step 1	Install the Linux client.	The Symantec Endpoint Protection Manager administrator provides you with the installation package for a managed client or sends you a link by email to download it. You can also uninstall an unmanaged client, which does not communicate with Symantec Endpoint Protection Manager in any way. The primary computer user must administer the client computer, update the software, and update the definitions. You can convert an unmanaged client to a managed client. <a href="#">Installing the Symantec Agent for Linux or the Symantec Endpoint Protection client for Linux</a>
Step 2	Check that the Linux client communicates with Symantec Endpoint Protection Manager.	Double-click the Symantec Endpoint Protection shield. If the client successfully communicates with Symantec Endpoint Protection Manager, then server information displays under <b>Management</b> , next to <b>Server</b> . If you see <b>Offline</b> , then contact the Symantec Endpoint Protection Manager administrator. If you see <b>Self-managed</b> , then the client is unmanaged. The shield icon also indicates both the management and the communication status.
Step 3	Verify Auto-Protect is running.	Double-click the Symantec Endpoint Protection shield. Auto-Protect's status displays under <b>Status</b> , next to <b>Auto-Protect</b> . You can also check the status of Auto-Protect through the command-line interface: <code>sav info -a</code>
Step 4	Check that the definitions are up to date.	LiveUpdate automatically launches after installation is complete. You can verify that definitions are updated when you double-click the Symantec Endpoint Protection shield. The date of the definitions displays under <b>Definitions</b> . By default, LiveUpdate for the Linux client runs every four hours. If the definitions appear outdated, you can click <b>LiveUpdate</b> to run LiveUpdate manually. You can also use the command-line interface to run LiveUpdate: <code>sav liveupdate -u</code>
Step 5	Run a scan.	By default, the managed Linux client scans all files and folders daily at 12:30 A.M. However, you can launch a manual scan using the command-line interface: <code>sav manualscan -s pathname</code> <b>Note:</b> The command to launch a manual scan requires superuser privileges.

## [Symantec Endpoint Protection for Linux Frequently Asked Questions \(SEP for Linux FAQ\)](#)

### About auto-compile for the Symantec Endpoint Protection client for Linux

(For 14.3 MP1 and earlier)

The Symantec Endpoint Protection installer for Linux auto-compiles the Auto-Protect kernel module when the operating system kernel is incompatible with the pre-compiled Auto-Protect kernel modules.

Near the end of the installation process, if the client installer detects no active Auto-Protect modules, it launches the auto-compiler to compile the compatible modules.

Previously, Auto-Protect only functioned when the Linux computer's operating system ran a supported kernel. Alternately, you can manually compile the Auto-Protect kernel module.

#### Prerequisites

Development tools must be present on the Linux client computer for auto-compile to function, such as:



- 
- kernel-devel
  - kernel-source
  - linux-headers
  - build-essentials
  - "Development Tools"

Symantec Endpoint Protection kernel modules may not successfully compile on those Linux kernels whose source has been changed. Such Linux kernels are not supported through this feature.

### Using auto-compile

Auto-compile automatically launches during installation if needed. You do not need to take any action to launch auto-compile.

If the auto-compile process successfully completes, the terminal window displays the following:

Build Auto-Protect kernel modules from source code successfully

Custom drivers for symap and symev that the auto-compile process creates include **custom** in the file name. The file `sepf1-install.log` also confirms that auto-compile has run and succeeded. By default, this file is saved to `~/`.

If the auto-compile process fails, Auto-Protect installs but remains disabled. The terminal window displays a message similar to the following:

Build Auto-Protect kernel modules from source code failed with error: Number

Number represents the number of the error code, which varies. Refer to your compiler's documentation for information on any error code you receive.

## About the Linux client graphical user interface

(For 14.3 MP1 and earlier)

### NOTE

Symantec Agent for Linux 14.3 RU1 does not have a graphical user interface.





If your Linux computer includes a graphical user interface (GUI), the Symantec Endpoint Protection for Linux client displays a yellow shield notification area icon on the status tray. The icon provides information about whether the client is connected to a management server and the protection status.

You perform most management tasks using the command-line interface. However, you can use the Symantec Endpoint Protection client GUI to perform the following tasks:

- Review information about the version of the product and the virus definitions.
- Check the status of the client's protection, which includes whether Auto-Protect is enabled, and the status of any scheduled scans or manual scans.
- Run LiveUpdate to get the latest virus definitions and product updates.
- Get information about whether the client is unmanaged, or is managed and connects to Symantec Endpoint Protection Manager to receive updated policies.

You can also perform these tasks from the command line.

**Table 21: Symantec Endpoint Protection for Linux client status icons**

Icon	Description
	The client is unmanaged and functions correctly. The icon is a plain yellow shield.
	The client is managed, functions correctly, and successfully communicates with Symantec Endpoint Protection Manager. The icon is a yellow shield with a green dot.
	The client is managed, functions correctly, and does not successfully communicate with Symantec Endpoint Protection Manager. The icon is a yellow shield with a light yellow dot that contains a black exclamation mark.
	The client fails to function correctly because of disabled components, such as Auto-Protect, the real-time scanning service (rtvscand), or the client management service (smcd). The icon is a yellow shield with a white dot outlined in red and a red slash across the dot.

[Getting started on the Linux client](#)

## Installing Symantec Endpoint Protection clients with Remote Push

Remote Push pushes the client software to the computers that you specify, either by IP address or by computer names. Once the package copies to the target computer, the package installs automatically. The computer user does not need to begin the installation or to have administrator privileges.

**Remote Push comprises the following tasks:**

- You select an existing client installation package, create a new installation package, or create a package to update communication settings.
- For new installation packages, you configure and create the installation package.
- You specify the computers on your network to receive a package from Symantec Endpoint Protection Manager. Remote Push locates either specific computers for which you provide an IP number or range, or all computers that are visible by browsing the network.

### NOTE

To push the client installation package to Mac clients in the **Browse Network** tab, you must install the Bonjour service on the Symantec Endpoint Protection Manager server. See the following article:

[Installing the Bonjour Service for Symantec Endpoint Protection Manager 12.1.5 or later](#)

The Bonjour service does not support IPv6 networking. Macs that only have IPv6 networking enabled cannot display in **Browse Network**.

IPv6 networking is supported as of 14.2.

- Symantec Endpoint Protection Manager pushes the client software to the specified computers. The installation automatically begins on the computers once the package successfully copies to the target computer.

### NOTE

You cannot install the Linux client with Remote Push.

To install Symantec Endpoint Protection clients with Remote Push

1. In the console, launch the **Client Deployment Wizard**.

Click **Help > Getting Started Page** and then under **Required tasks**, click **Install the client software on your computers**.

---

2. In the **Client Deployment Wizard**, do one of the following tasks:

- Click **New Package Deployment** to create a new installation package, and then click **Next**.
- Click **Existing Package Deployment** to use a package that was previously created, and then click **Browse** to locate the package to install.  
The Client Deployment Wizard uploads the package and directs you to the **Computer Selection** panel (step 5).
- Under **Communication Update Package Deployment**, choose whether to update Windows or Mac client communication settings on the computers that already have the Symantec Endpoint Protection client installed. Follow the on-screen instructions, and then go to step 4.  
Use this option to convert an unmanaged client to a managed client.

#### [Restoring client-server communications with Communication Update Package Deployment](#)

3. For a new package, in the **Select Group and Install Feature Sets** panel, make selections from the available options, which vary depending on the installation package type. Click **Next**.

#### **NOTE**

To uninstall existing security software on the Windows client, you must configure custom Client Install Settings before you launch the Client Deployment Wizard. You can also use an existing client install package that is configured to enable this function.

#### [Configuring client packages to uninstall existing security software](#)

#### [About the Windows client installation settings](#)

4. Click **Remote Push**, and then click **Next**.

5. In the **Computer Selection** panel, locate the computers to receive the software using one of the following methods:

- To browse the network for computers, click **Browse Network**.
- To find computers by IP address or computer name, click **Search Network**, and then click **Find Computers**.

You can set a timeout value to constrain the amount of time that the server applies to a search.

6. Click > > to add the computers to the list, and authenticate with the domain or workgroup if the wizard prompts you.

The remote push installation requires elevated privileges. If the client computer is part of an Active Directory domain, you should use a domain administrator account.

7. Click **Next**, and then click **Send** to push the client software to the selected computers.

Once the **Deployment Summary** panel indicates a successful deployment, the installation starts automatically on the client computers.

The installation takes several minutes to complete.

8. Click **Next**, and then click **Finish**.

9. Confirm the status of the installed clients on the **Clients** page.

For new Symantec Endpoint Protection installations, the client computers may not appear within Symantec Endpoint Protection Manager until after they restart, either automatically or by action you or the user takes.

#### [Restarting the client computers from Symantec Endpoint Protection Manager](#)

#### [Running a report on the deployment status of clients](#)

#### **NOTE**

After you remotely install the client installation package to Mac clients, you must verify on the client computer that the kernel extension is authorized. Kernel extension authorization is required for Symantec Endpoint

---

Protection to fully function, and Remote Push does not prompt you to authorize if authorization is needed. On the Mac, check the **Security & Privacy** system preference, and click **Allow**.

[Preparing for client installation](#)

[Preparing Windows and Mac computers for remote deployment](#)

[Choosing which security features to install on the client](#)

[Choosing a method to install the client using the Client Deployment Wizard](#)

## Installing Symantec Endpoint Protection clients with Web Link and Email

The Web Link and Email option creates the installation package and the URL for the installation package. The users receive the URL in an email to download the package and install the Symantec Endpoint Protection client. Users must have administrator privileges to install the package.

**Web Link and Email comprises the following tasks:**

- You select, configure, and then create the client installation package.  
You choose from the options that appear for the configuration of Windows, Mac, and Linux client installation packages. All client installation packages are stored on the computer that runs Symantec Endpoint Protection Manager.
- Email from Symantec Endpoint Protection Manager notifies the computer users that they can download the client installation package.  
You provide a list of users to receive an email message, which contains instructions to download and install the client installation package. Users follow the instructions to install the client software.

### NOTE

The Mac and the Linux client install packages automatically export a .zip archive file format. To correctly preserve the file permissions, you should expand the archive file with a native archive program, such as the Mac Archive Utility or the ditto command. You cannot use the Mac unzip command, a third-party application, or any Windows application to expand the files for these operating systems.

Before you use Web Link and Email, make sure that you correctly configure the connection from the management server to the mail server.

[Establishing communication between the management server and email servers](#)

To install Symantec Endpoint Protection clients with Web Link and Email

1. In the console, launch the **Client Deployment Wizard**.

Click **Help > Getting Started Page** and then under **Required tasks**, click **Install the client software on your computers**.

2. In the **Client Deployment Wizard**, click **New Package Deployment**, and then click **Next**. Web Link and Email only sends a new installation package.
3. Make selections from the available options, which vary depending on the installation package type, and then click **Next**.

### NOTE

To uninstall existing security software on the Windows client, you must configure custom Client Install Settings before launching the Client Deployment Wizard.

[Configuring client packages to uninstall existing security software](#)

[About the Windows client installation settings](#)

---

4. Click **Web Link and Email**, and then click **Next**.

5. In the **Email Recipients and Message** panel, specify the email recipients and the subject.

To specify multiple email recipients, type a comma after each email address. A management console system administrator automatically receives a copy of the message.

You can accept the default email subject and body, or edit the text. You can also copy the URL and post it to a convenient and secure online location, like an intranet page.

6. To create the package and deliver the link by email, click **Next**, and then click **Finish**.

7. Confirm that the computer users received the email message and installed the client software.

Client computers may not appear within Symantec Endpoint Protection Manager until after they restart, either automatically or by action you or the user takes. Mac clients automatically prompt a restart when installation completes. Linux clients do not require a restart.

[Restarting the client computers from Symantec Endpoint Protection Manager](#)

[Running a report on the deployment status of clients](#)

[Choosing which security features to install on the client](#)

[Choosing a method to install the client using the Client Deployment Wizard](#)

[Preparing for client installation](#)

## What do I do after I install the management server?

The following table displays the tasks to perform after you install and configure the product to assess whether the client computers have the correct level of protection. Continue to perform these tasks regularly, on a weekly or monthly basis.

**Table 22: Tasks to perform after you install**

Action	Description
Modify the Virus and Spyware Protection policy	<p><b>Change the following default scan settings:</b></p> <ul style="list-style-type: none"><li>• If you create a group for servers, change the scheduled scan time to a time when most users are offline. <a href="#">Setting up scheduled scans that run on Windows computers</a></li><li>• Enable Risk Tracer in Auto-Protect. For more information, see the article: <a href="#">What is Risk Tracer?</a> Risk Tracer has the following prerequisites:<ul style="list-style-type: none"><li>— Network Threat Protection is enabled. <a href="#">Running commands on client computers from the console</a></li><li>— Windows File and Printer Sharing is enabled. <a href="#">Customizing Auto-Protect for Windows clients</a></li></ul></li></ul>
Modify the Firewall policy for the remote computers group and the servers group	<ul style="list-style-type: none"><li>• Increase the security for remote computers by making sure that the following default firewall rules for an off-site location are enabled:<ul style="list-style-type: none"><li>— <b>Block Local File Sharing to external computers</b></li><li>— <b>Block Remote Administration</b></li></ul></li><li>• Decrease the security for the servers group by making sure that the following firewall rule is enabled: <b>Allow Local File Sharing to local computers</b>. This firewall rule ensures that only local traffic is allowed. <a href="#">Customizing firewall rules</a> <a href="#">Managing locations for remote clients</a></li></ul>

Action	Description
Exclude applications and files from being scanned	<p>You can increase performance by configuring the client not to scan certain folders and files. For example, the client scans the mail server directory every time a scheduled scan runs. You should exclude mail server program files and directories from being scanned.</p> <p>For more information, see the article: <a href="#">About the automatic exclusion of files and folders for Microsoft Exchange server and Symantec products</a>.</p> <p>You can improve performance by excluding the folders and files that are known to cause problems if they are scanned. For example, Symantec Endpoint Protection should not scan the proprietary Microsoft SQL Server files. You should add an exception that prevents scanning of the folders that contain the SQL Server database files. These exceptions improve performance and avoid corruption or files being locked when SQL Server must use them.</p> <p>For more information, see the knowledge base article: <a href="#">How to exclude MS SQL files and folders using Centralized Exceptions</a>.</p> <p>In addition, you should exclude false positives from scans.</p> <p>You can also exclude files by extension for Auto-Protect scans on Windows computers.</p> <p><a href="#">Creating exceptions for Virus and Spyware scans</a></p> <p><a href="#">Customizing Auto-Protect for Windows clients</a></p> <p><a href="#">Customizing Auto-Protect for Mac clients</a></p>
Run a quick report and scheduled report after the scheduled scan	<p>Run the quick reports and scheduled reports to see whether the client computers have the correct level of security.</p> <p><a href="#">About the types of Symantec Endpoint Protection Manager reports</a></p> <p><a href="#">Running and customizing quick reports</a></p> <p><a href="#">How to run scheduled reports</a></p>
Check to ensure that scheduled scans have been successful and clients operate as expected	<p>Review monitors, logs, and the status of client computers to make sure that you have the correct level of protection for each group.</p> <p><a href="#">Monitoring endpoint protection</a></p>
Assess your content storage and client communication bandwidth requirements	<p>Symantec Endpoint Protection Manager stores the latest full version plus incremental deltas only. This approach means that clients almost always download deltas, not full packages. Only in the rare case where a client is extremely out of date (more than three months), is a full download of the latest content required.</p> <p>If your environment must control network bandwidth precisely, you can also throttle client communication. For more information, see the article: <a href="#">Symantec Endpoint Protection Bandwidth Control for Client Communication</a></p> <p><a href="#">How to update content and definitions on the clients</a></p> <p>For more information about calculating storage and bandwidth needs, see the <a href="#">Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper</a>.</p>
Configure notifications for a single risk outbreak and when a new risk is detected	<p>Create a notification for a <b>Single risk event</b> and modify the notification for <b>Risk Outbreak</b>.</p> <p>For these notifications, Symantec recommends that you do the following actions:</p> <ol style="list-style-type: none"> <li>1. Change the <b>Risk severity</b> to <b>Category 1 (Very Low and above)</b> to avoid receiving emails about tracking cookies.</li> <li>2. Keep the <b>Damper</b> setting at <b>Auto</b>.</li> </ol> <p>Notifications are critical to maintaining a secure environment and can also save you time.</p> <p><a href="#">Setting up administrator notifications</a></p> <p><a href="#">Managing notifications</a></p>

[Getting up and running on Symantec Endpoint Protection for the first time](#)

See: [Symantec Endpoint Protection Recommended Best Practices for Securing an Enterprise Environment](#)

---

## Communication ports for Symantec Endpoint Protection

If the computers that run Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client also run third-party firewall software or hardware, you must open certain ports. These ports are for remote deployment and for communication between the management server and clients. See your firewall product documentation for instructions to open ports or allow applications to use ports.

By default, the firewall component of Symantec Endpoint Protection already allows traffic on these ports.

### WARNING

The firewall in the Symantec Endpoint Protection client is disabled by default at initial installation until the computer restarts. To ensure firewall protection, leave the Windows firewall enabled on the clients until the software is installed and the client is restarted. The Symantec Endpoint Protection client firewall automatically disables the Windows firewall when the computer restarts.

**Table 23: Ports for client and server installation and communication**

Protocol and port number	Used for	Listening process	Description	Applicable versions
TCP 139, 445 UDP 137, 138	Push deployment from Symantec Endpoint Protection Manager to Windows computers	svchost.exe	<ul style="list-style-type: none"><li>Initiated by Symantec Endpoint Protection Manager (clientremote.exe)</li><li>Not configurable</li></ul> Also uses TCP ephemeral ports.	All
TCP 22	Push deployment from Symantec Endpoint Protection Manager to Mac computers	launchd	<ul style="list-style-type: none"><li>Initiated by Symantec Endpoint Protection Manager (clientremote.exe)</li><li>Not configurable</li></ul>	All
TCP 2967	Group Update Provider (GUP) web-caching proxy functionality	ccSvcHst.exe	<ul style="list-style-type: none"><li>Initiated by Symantec Endpoint Protection clients</li><li>Configurable</li></ul>	All
TCP 2968	Web and Cloud Access Protection Client Authentication	ccSvcHst.exe	<ul style="list-style-type: none"><li>Initiated by Symantec Endpoint Protection clients</li><li>Configurable</li></ul>	14.2 and later
TCP 2638	Communication between the automatically installed database and Symantec Endpoint Protection Manager	<ul style="list-style-type: none"><li>sqlserver.exe (SQL Server Express database; 14.3 RU1 and later)</li><li>dbsrv16.exe (embedded database; 14.3 MP1 and earlier)</li></ul>	<ul style="list-style-type: none"><li>Initiated by Symantec Endpoint Protection Manager</li><li>Configurable</li></ul>	All
TCP 1433	Communication between a remote SQL Server database and Symantec Endpoint Protection Manager	sqlserver.exe	<ul style="list-style-type: none"><li>Initiated by Symantec Endpoint Protection Manager</li><li>Configurable</li></ul> The Symantec Endpoint Protection Manager management server also uses TCP ephemeral ports.	All

Protocol and port number	Used for	Listening process	Description	Applicable versions
TCP 8443	Server communication (HTTPS)	SemSvc.exe	All logon information and administrative communication takes place using this secure port. <ul style="list-style-type: none"> <li>Initiated by the Java-based remote console or web-based remote console, or by replication partners</li> <li>Configurable</li> </ul> Symantec Endpoint Protection Manager listens on this port.	All
TCP 9090	Web console communication	SemSvc.exe	This port is used only for initial HTTP communication between the remote management console and Symantec Endpoint Protection Manager. This initial communication includes installation, and to display the logon screen only. <ul style="list-style-type: none"> <li>Initiated by the remote Web console</li> <li>Configurable</li> </ul> Also uses TCP ephemeral ports.	All
TCP 8014	Communication between Symantec Endpoint Protection Manager (HTTP) and the Symantec Endpoint Protection client	httpd.exe (Apache)	<ul style="list-style-type: none"> <li>Initiated by Symantec Endpoint Protection clients</li> <li>Configurable</li> </ul> Clients also use TCP ephemeral ports.	All
TCP 443	Communication between the Symantec Endpoint Protection Manager (HTTPS) and the Symantec Endpoint Protection client	httpd.exe (Apache)	<ul style="list-style-type: none"> <li>Initiated by Symantec Endpoint Protection clients</li> <li>Configurable</li> </ul> Clients also use TCP ephemeral ports.	All
TCP 443	Communication between the Symantec Endpoint Protection Manager and the cloud console	prunsvr.exe	For information on which domains to add to the proxy bypass list for the cloud console, see: <a href="#">Proxy error messages appear in the Endpoint Protection Manager Cloud tab &gt; Troubleshooting</a>	All
HTTPS 443	Communication between the Symantec Endpoint Protection roaming client and the cloud console	None	Managed clients that have intermittent communication with Symantec Endpoint Protection Manager upload their critical events directly to the cloud console. Symantec Endpoint Protection Manager must be enrolled with the cloud console. <a href="#">Monitoring roaming Symantec Endpoint Protection clients from the cloud console</a>	14.2 and later
HTTP 8081 HTTPS 8082	Communication between Symantec Endpoint Protection Manager and the Content Analysis server appliance	Symantec Endpoint Protection Manager	The management server uses this port to communicate with the Content Analysis server or the Malware Analysis Appliance.	14.2.x versions only. Deprecated in 14.3.
TCP 8445	Used by the remote reporting console	httpd.exe (Apache)	<ul style="list-style-type: none"> <li>Initiated by the reporting console</li> <li>Configurable</li> </ul>	All



Protocol and port number	Used for	Listening process	Description	Applicable versions
TCP 8446	Web services	semapisrv.exe	Remote management applications use this port to send web services traffic over HTTPS. <ul style="list-style-type: none"> <li>Initiated by Remote Monitoring and Management (RMM) and by EDR</li> <li>Configurable</li> <li>Used for Java Remote Console</li> </ul>	All
TCP 8447	Process launcher	semlaunchsrv.exe	This virtual service account launches any Symantec Endpoint Protection Manager processes that require higher privileges, so that these other services do not need to have them. Only honors requests from localhost. <ul style="list-style-type: none"> <li>Initiated by Symantec Endpoint Protection Manager (SemSvc.exe)</li> <li>Configurable</li> </ul>	All
TCP 8765	Server control	SemSvc.exe	Used by Symantec Endpoint Protection Manager for Tomcat web service for shutdown. <ul style="list-style-type: none"> <li>Initiated by Symantec Endpoint Protection Manager</li> <li>Configurable</li> </ul>	All
TCP 1100	Remote object registry	SemSvc.exe	Tells AjaxSwing on which port to run RMI Registry. <ul style="list-style-type: none"> <li>Initiated by AjaxSwing</li> <li>Not configurable</li> </ul>	All
UDP 514	Forwarding data to a Syslog server (Optional)	SemSvc.exe	<ul style="list-style-type: none"> <li>Outbound traffic from Syslog server to Symantec Endpoint Protection Manager</li> <li>Inbound traffic to Syslog server</li> <li>Configurable</li> </ul> Traffic to or from Symantec Endpoint Protection Manager uses UDP ephemeral ports.	

- Windows Vista and later contain a firewall that is enabled by default. If the firewall is enabled, you might not be able to install or deploy the client software remotely. If you have problems deploying the client to computers running these operating systems, configure their firewalls to allow the required traffic.
- If you decide to use the Windows firewall after deployment, you must configure it to allow file and printer sharing (port 445).

For more information about configuring Windows firewall settings, see the Windows documentation.

[About basic management server settings](#)

[Preparing Windows and Mac computers for remote deployment](#)

[Monitoring endpoint protection](#)

[Preparing for client installation](#)

---

# Installing and Uninstalling the Management Server and Clients

---

Plan your installation of Symantec Endpoint Protection Manager and the clients.

Before you install the Symantec Endpoint Protection Manager, you may need to consider the following issues:

- The number of clients in your network.
- Which database you want to use, either the default Microsoft SQL Server Express database or Microsoft SQL Server.
- Whether to set up multiple sites.
- Whether to set up a failover server.

Before you install the Symantec Endpoint Protection clients, you may need to consider the following issues:

- Which features you want to install.
- Which deployment method you want to use.

## Network architecture considerations

You can install Symantec Endpoint Protection for testing purposes without considering your company network architecture. You can install Symantec Endpoint Protection Manager with a few clients, and become familiar with the features and functions.

When you are ready to install the production clients, you should plan your deployment based on your organizational structure and computing needs.

**You should consider the following elements when you plan your deployment:**

- Symantec Endpoint Protection Manager  
Administrators use Symantec Endpoint Protection Manager to manage security policies and client computers. You may want to consider the security and availability of the computer on which Symantec Endpoint Protection Manager is installed.
- Remote console  
Administrators can use a remote computer that runs the console software to access Symantec Endpoint Protection Manager. Administrators may use a remote computer when they are away from the office. You should ensure that remote computers meet the remote console requirements.
- Local and remote computers  
Remote computers may have slower network connections. You may want to use a different installation method than the one you use to install to local computers.
- Portable computers such as notebook computers  
Portable computers may not connect to the network on a regular schedule. You may want to make sure that portable computers have a LiveUpdate policy that enables a LiveUpdate schedule. Any portable computers that do not check in regularly do not get other policy updates.
- Computers that are located in secure areas  
Computers that are located in secure areas may need different security settings from the computers that are not located in secure areas.

You identify the computers on which you plan to install the client. Symantec recommends that you install the client software on all unprotected computers, including the computer that runs Symantec Endpoint Protection Manager.

[Getting up and running on Symantec Endpoint Protection for the first time](#)

## About choosing a database type

Symantec Endpoint Protection Manager uses a database to store information about clients and settings. The database is created as part of the configuration process. You must decide which database to use before you install the management server. You cannot use the console until you have configured the management server to use a database.

**Table 24: Databases that Symantec Endpoint Protection Manager uses**

Database type	Description
Microsoft SQL Server Express (default)	The SQL Server Express database is automatically installed with Symantec Endpoint Protection Manager by default. The SQL Server Express database does not require configuration and is easier to install than the SQL Server. You can also install SQL Server Express separately, which does require some configuration. The SQL Server Express database supports up to 5,000 clients. In 14.3 MP1 and earlier versions, the default database was the embedded database. <a href="#">About basic management server settings</a>
Embedded database	The embedded database is automatically installed with Symantec Endpoint Protection Manager by default. The embedded database does not require configuration. The embedded database supports up to 5,000 clients.
Microsoft SQL Server	If you choose to use this option, you must install SQL Server and SQL Server Native Client before you install Symantec Endpoint Protection Manager. For optimal compatibility, you install the version of SQL Server Native Client equal to your version of SQL Server. You should consider purchasing and installing SQL Server for the following reasons: <ul style="list-style-type: none"><li>• You must support more than 5,000 clients. Each management server that uses SQL Server can support up to 18,000 clients. If your organization has more clients, you can install another management server.</li><li>• You want to support failover and load balancing.</li><li>• You want to set up additional management servers as site partners.</li></ul> <a href="#">Determining how many sites you need</a> If you create a SQL Server database, you must first install an instance of SQL Server on either a local or a remote server. You must then configure it for communication with the management server. <a href="#">About SQL Server configuration settings</a>

## About basic management server settings

The following values represent the default settings when you install the Symantec Endpoint Protection Manager.

You can configure some of the following values only when you install the Symantec Endpoint Protection Manager using a custom configuration.

[Installing Symantec Endpoint Protection Manager](#)

[Communication ports for Symantec Endpoint Protection](#)

**Table 25: Basic server settings**

Setting	Default	Description
Site Name	My Site (default) Site local host name (custom)	The name of the site as it appears in Symantec Endpoint Protection Manager. Site name is the highest-level container under which all features are configured and run within Symantec Endpoint Protection Manager.
Server name	local host name	The name of the computer that runs Symantec Endpoint Protection Manager.

Setting	Default	Description
Server data folder	SEPM_Install\data	The directory in which the Symantec Endpoint Protection Manager places data files including backups, replicated logs, and other files. The installer creates this directory if it does not exist. The default value for SEPM_Install is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager.
Encryption password	None	This password encrypts communication between Symantec Endpoint Protection Manager and clients. If you choose the default configuration, the system automatically generates the encryption password for you. From the summary screen, you can print or copy this information to the clipboard. If you choose a custom configuration, you can have the system automatically generate a random password, or you can create your own password. The password can be from 6-32 alphanumeric characters. Document this password and put it in a secure location. You cannot change or recover the password after you create the database. You must also enter this password for disaster recovery purposes if you do not have a backed-up database to restore. <a href="#">Disaster recovery best practices for Endpoint Protection</a>
User name	admin	The name of the default user that is used to log on to the Symantec Endpoint Protection Manager console for the first time. This value is not configurable.
Password	None	The password that is specified for the admin account during server configuration. You need the original admin password to reconfigure the management server at a later time. Document this password and put it in a secure location.
Email address	None	System notifications are sent to the email address specified.

## About SQL Server configuration settings

If you install Symantec Endpoint Protection Manager with a SQL Server database, there are specific configuration requirements for SQL Server.

Before you create the database, Symantec recommends that you install a new instance of SQL Server that conforms to Symantec installation and configuration requirements. You can install a database in an existing instance, but the instance must be configured properly or your database installation fails. For example, if you select a case-sensitive SQL collation, your installation fails.

### WARNING

To maximize the security posture of remote SQL Server communications, place both servers in the same secure subnet.

**Table 26: Required SQL Server configuration settings**

Configuration setting	Installation requirement
Instance name	Do not use the default instance name. Create a name such as SEPM. By default, a database named Sem5 is created in the SQL Server instance when you install Symantec Endpoint Protection Manager. The default name is supported, but can cause confusion if you install multiple instances on one computer.
Authentication configuration	Mixed mode or Windows Authentication mode <a href="#">About SQL Server database authentication modes</a>
sa password	Set this password when you set Mixed Mode authentication.
Enabled protocol	TCP/IP

Configuration setting	Installation requirement
IP addresses for TCP/IP	Enable IP1 and IP2
TCP/IP port numbers for IP1, IP2, and IPALL	Set TCP Dynamic Ports to blank, and specify a TCP port number. The default port is typically 1433. You specify this port number when you create the database. The Symantec Endpoint Protection Manager database does not support dynamic ports.
Remote connections	Must be enabled. TCP/IP protocol must also be specified.

If your database is located on a remote server, you must also install SQL Server client components on the computer that runs Symantec Endpoint Protection Manager. SQL Server client components include `BCP.EXE`. The version number of the SQL Server client components should be the same as the version number of SQL Server that you use. Refer to your SQL Server documentation for installation instructions.

During the Symantec Endpoint Protection Manager database configuration phase of the installation, you select and enter various database values. Understand the decisions you must make to correctly configure the database.

The following table displays the settings that you might need to know before you begin the installation process.

**Table 27: SQL Server database settings**

Setting	Default	Description
Server name	local host name	Name of the computer that runs Symantec Endpoint Protection Manager.
Server data folder	SEPM_Install\data	Folder in which the Symantec Endpoint Protection Manager places data files including backups, replication, and other Symantec Endpoint Protection Manager files. The installer creates this folder if it does not exist. The default value for SEPM_Install is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager.
Encryption password	None	The password that encrypts communication between Symantec Endpoint Protection Manager and clients. The password can be from 6-32 alphanumeric characters and is required. Document this password and put it in a secure location. You cannot change or recover the password after you create the database. You must also enter this password for disaster recovery purposes if you do not have a backed-up database to restore. <a href="#">Disaster recovery best practices for Endpoint Protection</a>

Setting	Default	Description
Database server	local host name	Name of the computer where SQL Server is installed, and the optional instance name. If the database server was installed with the default instance, which is no name, type either host name or the host's IP address. If the database server was installed with a named instance, type either host name\instance_name or IP address\instance_name. The use of host name only works with properly configured DNS. If you install to a remote database server, you must first install the SQL Server client components on the computer that runs Symantec Endpoint Protection Manager.
SQL Server Port	1433	The port that is used to send and receive traffic to the SQL Server. The use of port 0 is not supported. Port 0 specifies a random, negotiated port.
Database Name	sem5	Name of the database that is created.
Database user name	sem5	Name of the database user account that is created. The user account has a standard role with read and write access. The name can be a combination of alphanumeric values and the special characters ~ # % _ + =   : . . The special characters ` ! @ ' \$ ^ & * ( ) - { } [ ] " \ / < ; > , ? are not allowed. The following names are also not allowed: sysadmin, server admin, setupadmin, securityadmin, processadmin, dbcreator, diskadmin, bulkadmin.
Database password	None	The password that is associated with the database user account. The name can be a combination of alphanumeric values and the special characters ~ # % _ + =   : . /. The special characters ! @ * ( ) { } [ ] ; , ? are not allowed.
SQL Server native client folder	SQL Server 2008: Install directory\100\Tools\Binn SQL Server 2012: Install directory\110\Tools\Binn SQL Server 2014 / 2016 / 2017 / 2019: Install directory\Client SDK\ODBC\110\Tools\Binn	Location of the local SQL native client directory that contains bcp.exe. The installation paths that are shown represent the default paths for Microsoft SQL Server. Install directory represents the installation drive and directory for Microsoft SQL Server. To install the SQL Server native client, see the Microsoft TechNet page appropriate for your version of SQL Server: <a href="#">Installing SQL Server Native Client</a>
Server user name	None	Name of the database server administrator account, which is typically sa.
Server password	None	The password that is associated with the database server administrator account, which is typically sa.

Setting	Default	Description
Database data folder	<p>SQL Server 2008: Install directory\MSSQL10.MSSQLSERVER\MSSQL\Data</p> <p>SQL Server 2008 R2: Install directory\MSSQL10_50.MSSQLSERVER\MSSQL\Data</p> <p>SQL Server 2012: Install directory\MSSQL11.MSSQLSERVER\MSSQL\Data</p> <p>SQL Server 2014: Install directory\MSSQL12.MSSQLSERVER\MSSQL\Data</p> <p>SQL Server 2016: Install directory\MSSQL13.MSSQLSERVER\MSSQL\Data</p> <p>SQL Server 2017: Install directory\MSSQL14.MSSQLSERVER\MSSQL\Data</p> <p>SQL Server 2019: Install directory\MSSQL15.MSSQLSERVER\MSSQL\Data</p>	<p>Location of the SQL Server data folder. If you install to a remote server, the volume identifier must match the identifier on the remote server.</p> <p>The installation paths shown represent the default paths for Microsoft SQL Server.</p> <ul style="list-style-type: none"> <li>• If you install to a named instance on SQL Server 2008, the instance name is appended to MSSQL10. For example, \MSSQL10.instance name\MSSQL\Data</li> <li>• If you install to a named instance on SQL Server 2008 R2, the instance name is appended to MSSQL10_50. For example, \MSSQL10_50.instance name\MSSQL\Data</li> <li>• If you install to a named instance on SQL Server 2012, the instance name is appended to MSSQL11. For example, \MSSQL11.instance name\MSSQL\Data</li> <li>• If you install to a named instance on SQL Server 2014, the instance name is appended to MSSQL12. For example, \MSSQL12.instance name\MSSQL\Data</li> <li>• If you install to a named instance on SQL Server 2016, the instance name is appended to MSSQL13. For example, \MSSQL13.instance name\MSSQL\Data</li> <li>• If you install to a named instance on SQL Server 2017, the instance name is appended to MSSQL14. For example, \MSSQL14.instance name\MSSQL\Data</li> <li>• If you install to a named instance on SQL Server 2019, the instance name is appended to MSSQL15. For example, \MSSQL15.instance name\MSSQL\Data</li> </ul> <p><a href="#">File Locations for Default and Named Instances of SQL Server</a></p> <p><b>Note:</b> Clicking <b>Default</b> displays the correct installation folder if you entered the database server and instance name correctly. If you click <b>Default</b> and the correct installation folder does not appear, your database creation fails.</p>

## Installing Symantec Endpoint Protection Manager

# About SQL Server database authentication modes

The Symantec Endpoint Protection Manager supports two modes of SQL Server database authentication:

- Windows Authentication mode
- Mixed mode

SQL Server can be configured to use either Windows Authentication or mixed mode authentication. Mixed mode authentication allows the use of either Windows or SQL Server credentials. When SQL Server is configured to use mixed mode, Symantec Endpoint Protection Manager may be set to use either Windows Authentication or mixed mode

---

authentication. When SQL Server is set to use Windows Authentication mode, Symantec Endpoint Protection Manager must also be configured to use Windows Authentication mode.

For the remote database connections that use the Windows Authentication mode, be aware of the following requirements:

- For deployments in an Active Directory environment, Symantec Endpoint Protection Manager and SQL Server must be located in the same Windows domain.
- For deployments in a Workgroup environment, the Windows account credentials must be the same for the local computers and the remote computers.

[About SQL Server configuration settings](#)

## Internationalization requirements

Certain restrictions apply when you install Symantec Endpoint Protection Manager in a non-English or mixed-language environment.

**Table 28: Internationalization requirements**

Component	Requirements
Computer names, server names, and workgroup names	<p>Non-English characters are supported with the following limitations:</p> <ul style="list-style-type: none"><li>• Network audit may not work for a host or user that uses a double-byte character set or a high-ASCII character set.</li><li>• Double-byte character set names or high-ASCII character set names may not appear properly on the Symantec Endpoint Protection Manager console or on the client user interface.</li><li>• A long double-byte or high-ASCII character set host name cannot be longer than what NetBIOS allows. If the host name is longer than what NetBIOS allows, the Home, Monitors, and Reports pages do not appear on the Symantec Endpoint Protection Manager console.</li></ul>
English characters	<p>English characters are required in the following situations:</p> <ul style="list-style-type: none"><li>• Deploy a client package to a remote computer.</li><li>• Define the server data folder in the Management Server Configuration Wizard.</li><li>• Define the installation path for Symantec Endpoint Protection Manager.</li><li>• Define the credentials when you deploy the client to a remote computer.</li><li>• Define a group name.</li></ul> <p>You can create a client package for a group name that contains non-English characters. You might not be able to deploy the client package using the Push Deployment Wizard when the group name contains non-English characters, however.</p> <ul style="list-style-type: none"><li>• Push non-English characters to the client computers.</li></ul> <p>Some non-English characters that are generated on the server side may not appear properly on the client user interface.</p> <p>For example, a double-byte character set location name does not appear properly on non-double-byte character set named client computers.</p>
User Information client computer dialog box	<p>Do not use double-byte or high-ASCII characters when you provide feedback in the <b>User Information</b> client computer dialog box after you install the exported package.</p> <p><a href="#">Collecting user information</a></p>
License Activation wizard	<p>Do not use double-byte characters in the following fields:</p> <ul style="list-style-type: none"><li>• First name</li><li>• Last name</li><li>• Company name</li><li>• City</li><li>• State/province</li></ul>



---

In 14.3 RU1 MP1 and earlier, the Symantec Endpoint Protection Manager and the Symantec Endpoint Protection Windows clients were translated from English into 12 languages: Chinese, Czech, French, German, Italian, Japanese, Korean, Polish, Brazilian Portuguese, Russian, and Spanish. In 14.3 RU2, Symantec Endpoint Protection was translated into 4 languages only: French, Japanese, Brazilian Portuguese, and Spanish.

## Uninstalling Symantec Endpoint Protection Manager

Uninstalling Symantec Endpoint Protection Manager uninstalls the server and console. You can optionally remove the database and the database backup files during uninstallation. To uninstall Symantec Endpoint Protection Manager, you use the Windows control panel for removing, repairing, or changing an application, typically **Programs and Features**.

If you plan to reinstall Symantec Endpoint Protection Manager, you should back up the database before you uninstall it.

In some cases, you may have to uninstall Symantec Endpoint Protection Manager using other methods, such as the CleanWipe utility. See:

[Uninstall Symantec Endpoint Protection](#)

[Backing up the database and logs](#)

## Managing the Symantec Endpoint Protection client installation

You must install a Symantec Endpoint Protection client on every computer you want to protect, whether the computer is physical or virtual.

**Table 29: Client computer installation tasks**

Action	Description
Step 1: Identify client computers	Identify the computers on which you want to install the client software. Check that all the computers run a supported operating system.  <b>Note:</b> Symantec recommends that you also install the client on the computer that hosts Symantec Endpoint Protection Manager.  For the most current system requirements, see: <a href="#">Release notes, new fixes, and system requirements for all versions of Endpoint Protection</a>
Step 2: Identify computer groups (optional)	Identify the computer groups to which you want the clients to belong. For example, you can group clients based on type of computer, to conform to your corporate organization, or to the security level required. You can create these groups before or after you install the client software. You can also import an existing group structure such as an Active Directory structure. <a href="#">Managing groups of clients</a> <a href="#">Importing existing groups and computers from an Active Directory or an LDAP server</a>
Step 3: Prepare client computers for deployment and installation	If your users do not have administrative rights for their computers, then you should remotely install the client software using Remote Push. The Remote Push installation requires you to enter the credentials that have local administrative rights for the computers. <a href="#">Installing Symantec Endpoint Protection clients with Remote Push</a> Prepare the computers for remote client deployment and for successful communication with Symantec Endpoint Protection Manager after installation. <a href="#">Preparing Windows and Mac computers for remote deployment</a>

Action	Description
Step 4: Determine features and deploy client software	<p>You deploy the client software using one of the available methods. You can also export a customized client package to deploy later or with a third-party tool.</p> <p><b>Note:</b> Symantec recommends that you do not perform third-party installations simultaneous to the installation of Symantec Endpoint Protection. The installation of any third-party programs that make network- or system-level changes may cause undesirable results when you install Symantec Endpoint Protection. If possible, restart the client computers before you install Symantec Endpoint Protection.</p> <p><a href="#">Choosing a method to install the client using the Client Deployment Wizard</a>  <a href="#">Exporting client installation packages</a>  <a href="#">Installing Windows client software using third-party tools</a></p> <ul style="list-style-type: none"> <li>You decide which features to install to the client computers. You configure custom client feature sets and installation settings before you export or deploy an installation package. Installation settings include the installation folder and the restart settings. You can also use the default client install feature sets and installation settings.  <a href="#">Choosing which security features to install on the client</a>  <a href="#">About the Windows client installation settings</a></li> <li>For Windows clients, you can choose to automatically uninstall existing third-party security software when you configure client installation settings.  <a href="#">Configuring client packages to uninstall existing security software</a></li> </ul>
Step 5: Verify installation status	<p>Confirm that the client installation succeeded and that clients communicate with Symantec Endpoint Protection Manager. Managed clients may not appear in the console until after they are restarted.  <a href="#">Symantec Endpoint Protection client status icons</a>  <a href="#">Restarting the client computers from Symantec Endpoint Protection Manager</a></p>

After installation, you can take additional steps to secure unmanaged computers and optimize the performance of your Symantec Endpoint Protection installation.

## Preparing Windows and Mac computers for remote deployment

Before you deploy Symantec Endpoint Protection from Symantec Endpoint Protection Manager, you must take steps to prepare the computers to ensure a successful remote installation. These steps pertain only to remote installation. You can reverse these changes afterward, but you must apply them again to perform another remote installation.

### NOTE

You cannot deploy the Symantec Endpoint Protection client to Linux computers remotely from Symantec Endpoint Protection Manager.

**Table 30: Tasks to prepare all computers for remote deployment**

Task	Details
Have administrative rights to your client computers	If the client computer is part of an Active Directory domain, you should use domain administrator account credentials for a remote push installation. Otherwise, have the administrator credentials available for each computer to which you deploy.
Modify firewall settings	<p>Modify firewall settings to allow communication between Symantec Endpoint Protection components.  <a href="#">Communication ports for Symantec Endpoint Protection</a></p>

Task	Details
Uninstall existing third-party security software	<p>Uninstall any third-party security software currently in use. For Windows computers, Symantec Endpoint Protection includes a tool to help automatically uninstall select third-party security software. You must separately uninstall any security software that this tool does not uninstall.</p> <p><b>Note:</b> Some programs may have special uninstallation routines, or may need to have a self-protection component disabled. See the documentation for the third-party software.</p> <p>You configure this tool before you deploy, and the uninstallation occurs before Symantec Endpoint Protection installs.</p> <p><a href="#">Configuring client packages to uninstall existing security software</a></p>
Uninstall Symantec Endpoint Protection clients that do not uninstall normally	<p>You can uninstall an existing installation of the Symantec Endpoint Protection client for Windows. You should only use this option if the existing Symantec Endpoint Protection installation does not uninstall normally. You should not use this option as part of a standard deployment.</p> <p>You configure this tool before you deploy, and the uninstallation occurs before Symantec Endpoint Protection installs.</p> <p><a href="#">Configuring client packages to uninstall existing security software</a></p>
Uninstall unsupported or consumer Symantec security software	<p>Uninstall any unsupported Symantec security software, such as Symantec AntiVirus or Symantec Client Security. Migration directly from these products is not supported.</p> <p>You must also uninstall any consumer-branded Symantec security products, such as Norton Internet Security.</p> <p>See the documentation for your Symantec software for information about uninstallation.</p> <p><a href="#">Supported upgrade paths to the latest version of Symantec Endpoint Protection 14.x</a></p>

**Table 31: Tasks to prepare Windows clients for remote deployment**

Operating system	Tasks
Prepare Windows Vista, Windows 7, or Windows Server 2008 / 2008 R2 computers	<p>Windows User Account Control blocks local administrative accounts from remotely accessing remote administrative shares such as C\$ and Admin\$. You do not need to fully disable User Account Control on the client computers during the remote deployment if you disable the registry key LocalAccountTokenFilterPolicy.</p> <p>To disable UAC remote restrictions, see:  <a href="http://support.microsoft.com/kb/951016">http://support.microsoft.com/kb/951016</a></p> <p>Perform the following tasks:</p> <ul style="list-style-type: none"> <li>• Disable the Sharing Wizard. The Sharing Wizard prevents more advanced sharing options from working during Remote Push.</li> <li>• Enable network discovery by using the Network and Sharing Center. Network discovery lets you browse the network. You do not need it to search the network.</li> <li>• Enable the built-in administrator account and assign a password to the account. Remote Push fails when the local administrator account has a blank password. If the Windows client computer is part of an Active Directory domain, use domain administrator account credentials with local administrator privileges for Remote Push.</li> <li>• Verify that the account with which you push the installation has administrator privileges.</li> <li>• Enable and start the Remote Registry service.</li> <li>• Disable or remove Windows Defender.</li> </ul> <p>Consult the operating system's documentation for guidance on how to successfully complete these tasks.</p>
Prepare Windows 8 / 8.1 or later, or Windows Server 2012 / 2012 R2 or later computers	<p>Before you deploy, perform the following tasks:</p> <ul style="list-style-type: none"> <li>• Disable the registry key LocalAccountTokenFilterPolicy. To disable UAC remote restrictions, see:  <a href="http://support.microsoft.com/kb/951016">http://support.microsoft.com/kb/951016</a></li> <li>• Enable and start the Remote Registry service.</li> <li>• Disable or remove Windows Defender.</li> </ul>

**Table 32: Tasks to prepare Mac clients for remote deployment**

Operating system	Tasks
Prepare the Mac computers on any supported operating system	<p>Before you deploy, perform the following tasks on the Mac computers:</p> <ul style="list-style-type: none"><li>Click <b>System Preferences &gt; Sharing &gt; Remote Login</b> and either allow access for all users, or only for specific users, such as Administrators.</li><li>If you use the Mac firewall, disable stealth mode. With stealth mode enabled, the remote push installation cannot discover the client through <b>Search Network</b>. To disable stealth mode on the Mac, see the following article and select your version of the Mac operating system. <a href="#">Use stealth mode to keep your Mac more secure</a></li><li>Ensure that the firewall does not block the port that Secure Shell (SSH) uses. By default, this port is TCP port 22. This port allows the required communication for remote logon.</li><li>The Bonjour service does not support IPv6 networking. To ensure that <b>Browse Network</b> or <b>Search Network</b> displays these Macs, ensure that they also have IPv4 networking enabled. IPv6 networking is supported as of 14.2.</li></ul>

[Communication ports for Symantec Endpoint Protection](#)

[Installing Symantec Endpoint Protection clients with Remote Push](#)

[Preparing for client installation](#)

## Choosing a method to install the client using the Client Deployment Wizard

After you install Symantec Endpoint Protection Manager, you install the Symantec Endpoint Protection client with the Client Deployment Wizard.

**Table 33: Client installation methods**

Options	Description
<b>Save Package</b>	<p>This installation option creates an executable installation package that you save on the management server and then distribute to the client computers. The users then install the client software, so they must have local administrator rights to their computers.</p> <p>You can install Windows, Mac, and Linux clients using this option.</p> <p><a href="#">Installing Symantec Endpoint Protection clients with Save Package</a></p>
<b>Remote Push</b>	<p>Remote push installation pushes the client software to the computers that you specify. The installation begins automatically on the client computers. Remote push installation does not require the user to have local administrator rights to their computers.</p> <p>You can install Windows and Mac clients using this option.</p> <p><a href="#">Installing Symantec Endpoint Protection clients with Remote Push</a></p> <p><a href="#">Preparing Windows and Mac computers for remote deployment</a></p>
<b>Web Link and Email</b>	<p>Users receive an email message that contains a link to download and install the client software. The users then install the client software, so they must have local administrator rights to their computers.</p> <p>You can install Windows, Mac, and Linux clients using this option.</p> <p><a href="#">Installing Symantec Endpoint Protection clients with Web Link and Email</a></p>

Before you run the Client Deployment Wizard, you review the installation options, optionally customize them, and then select those options during installation. Installation options include the protection technologies to install, the installation destination folder, and the restart behavior after installation.

[Choosing which security features to install on the client](#)

## Choosing which security features to install on the client

When you deploy the Windows client installation package with the Client Deployment Wizard, you must choose the feature set. The feature set specifies which protection features are installed on the client. You can select a default feature set or customize the feature set. Decide which feature set to install based on the role of the computers, and the level of security or performance that the computers need.

After installation, you should keep all features enabled.

**Table 34: Client installation feature sets (Windows)**

Feature set	Description
<b>Full Protection for Clients</b>	Recommended for workstations, desktop, and laptop computers. Includes all protection features. Appropriate for laptops, workstations, and desktops. Includes the full download protection and mail protocol protection. Whenever possible, use Full Protection for maximum security.
<b>Full Protection for Servers</b>	Recommended for servers. Includes all protection features except email scanner protection. Appropriate for any servers that require maximum network security, including the Symantec Endpoint Protection Manager server.
<b>Basic Protection for Servers</b>	Recommended for high-throughput servers. Includes Virus and Spyware Protection and Basic Download Protection. Since Intrusion Prevention may cause performance issues on high-throughput servers, this option is appropriate for any servers that require maximum network performance.

The Mac client installation package installs Virus and Spyware Protection and Intrusion Prevention. You cannot customize the features for the Mac client installation package.

The Linux client installation package only installs Virus and Spyware Protection.

### Customizing the feature set

If you want to install a subset of the protection features, create a custom feature set. However, Symantec recommends that you install all features.

You cannot customize the features for the Mac or Linux client installation package.

#### To create a custom client installation feature set:

1. In the console, click **Admin > Install Packages**.
2. Click **Client Install Feature Set > Add Client Install Feature Set**.
3. In the **Add Client Install Feature Set** dialog box, type a name and description, and check which protection features to install on the client.
4. Click **OK**.

## Managing client installation packages

To manage clients with Symantec Endpoint Protection Manager, you must export a managed client installation package, and then install the package files onto client computers. You can deploy the client with either Symantec Endpoint Protection Manager or a third-party deployment tool.

Symantec occasionally provides updated packages of installation files, usually when a new product version releases. You can automatically update the client software on all managed Windows and Mac clients in a group with the AutoUpgrade feature. You do not need to redeploy software with installation deployment tools.

**Table 35: Client installation package-related tasks**

Task	Description
Configure client installation packages	You can select specific client protection technologies to install and you can specify how the installation interacts with end users. <a href="#">Choosing which security features to install on the client</a> <a href="#">About the Windows client installation settings</a>
Export client installation packages	You can export packages for managed clients or unmanaged clients. You can export the packages as a single executable file or as a series of files in a directory. The method that you choose depends on your deployment method and whether you want to upgrade client software in groups. Typically, if you use Active Directory Group Policy Object, you do not choose to export to a single executable file. <a href="#">Exporting client installation packages</a> <a href="#">How to get an unmanaged client installation package</a> <a href="#">Installing an unmanaged Windows client</a>
Import client installation package updates	You can add updated client installation packages to the database to make them available for distribution from Symantec Endpoint Protection Manager. You can optionally export the packages during this procedure to make the package available for deployment to computers that do not have the client software. <a href="#">Importing client installation packages into Symantec Endpoint Protection Manager</a>
Upgrade Windows and Mac clients in one or more groups	You can install the exported packages to computers one at a time, or deploy the exported files to multiple computers simultaneously. When Symantec provides updates to client installation packages, you first add them to Symantec Endpoint Protection Manager and make them available for exporting. However, you do not have to reinstall them with client deployment tools. The easiest way to update Windows and Mac clients with the latest software is to use AutoUpgrade. You should first update a group with a small number of test computers. <a href="#">Upgrading client software with AutoUpgrade</a> You can also update clients with LiveUpdate if you permit clients to run LiveUpdate and if the LiveUpdate Settings policy permits updates.
Delete client installation packages	You can delete older client installation packages to save disk space. However, AutoUpgrade sometimes uses the older Windows client installation packages to build upgrade packages. The upgrade packages result in smaller downloads by clients.

## [Preparing for client installation](#)

### Exporting client installation packages

You might want to export a client install package if you need those options that are not available when you use **Save Package** in the **Client Deployment Wizard**. For example, you may need to create an unmanaged client with custom policies. You may also only need either 32-bit or 64-bit installation packages for Windows, or need either `DPKG` or `RPM` installation packages for Linux.

Once you export the client install package, you deploy it. **Remote Push** in the **Client Deployment Wizard** can deploy the Windows and Mac packages that you export. Alternately, you can install an exported package directly on to the client, or use a third-party program to deploy it.

You can create an installation package for managed clients or unmanaged clients. Both types of packages have the features, policies, and settings that you assign. If you create a package for managed clients, you can manage them with the Symantec Endpoint Protection Manager console. If you create a package for unmanaged clients, you cannot manage

---

them from the console. You can convert an unmanaged Windows or Mac client to a managed client at any time with **Communication Update Package Deployment** through the **Client Deployment Wizard**.

#### NOTE

If you export client installation packages from a remote console, the packages are created on the computer from which you run the remote console. Furthermore, if you use multiple domains, you must export the packages for each domain, or the clients do not appear in the correct domain groups.

To export client installation packages:

1. In the console, click **Admin**, and then click **Install Packages**.
2. Under **Install Packages**, click **Client Install Package**.
3. In the **Client Install Package** pane, under **Package Name**, right-click the package you want to export and then click **Export**.
4. Click **Browse** to navigate to and select the folder to contain the exported package, and then click **OK**.

#### NOTE

**Export Package** does not support directories with double-byte or high-ASCII characters, and blocks their selection.

5. Set the other options according to your installation goals. The options vary depending on the type and the platform of the installation package you export.

For details about the export options in this dialog box, click **Help**.

[Export Package settings](#)

6. Click **OK**.

[Importing client installation packages into Symantec Endpoint Protection Manager](#)

[Choosing which security features to install on the client](#)

[Restoring client-server communications with Communication Update Package Deployment](#)

## Importing client installation packages into Symantec Endpoint Protection Manager

You may need to import a client installation package into Symantec Endpoint Protection Manager if you upgrade to a newer version of Symantec Endpoint Protection Manager using a database that you have restored from a previous version. The database includes older client installation packages, and you need to import the newer packages.

You should always keep the Symantec Endpoint Protection Manager version the same or later than the client version.

#### NOTE

You can import an executable package such as .exe or .zip file packages directly, but it is not recommended. The .info file contains the information that describes the package and ensures proper migration to future builds of the Symantec Endpoint Protection client through delta updates. On the other hand, the Symantec Endpoint Protection Manager web console does not import the .info file format. In the web console, you can only import or export packages in a single file, such as in the .zip or .exe file format.

To import client installation packages into Symantec Endpoint Protection Manager

1. Copy the installation package that you import to a directory on the computer that runs Symantec Endpoint Protection Manager.

The client installation package consists of two files. One file is named `product_name.dat`, and the other file is named `product_name.info`. These files automatically import during the installation or upgrade of Symantec Endpoint Protection Manager. You can also get the packages from the `SEPM/Packages` folder of the installation file.

2. In the console, click **Admin > Install Packages**.
3. Under **Tasks**, click **Add a Client Install Package**.
4. In the **Add a Client Install Package** dialog box, type a name and a description for the package.
5. Click **Browse**.
6. In the **Select Folder** dialog box, locate and select the `product_name.info` file for the new package you copied in step 1, and then click **Select**.
7. When the **Completed successfully** prompt appears, click **Close**.

To export the installation files and make them available for deployment, click **Export this Package**, and then complete this procedure.

#### Exporting client installation packages

After you successfully import the package, you can see a "Package is created" event in the System > Administrative log. The event is described with text similar to "Successfully imported the SEP 14.3 RU2 64-bit package by Symantec Endpoint Protection Manager. This package is now available for deployment."

## Windows client installation package and content update sizes

Client installation packages, product patches, and content updates are also stored in the Symantec Endpoint Protection database and affect the storage requirements. Product patches contain information for client packages and information for each language or locale. Note that patches also create new, full client builds.

The following table displays the size of the client installation package if the maximum level of client logging and protection technologies are enabled.

**Table 36: Windows client installation package size**

Client type/ Definition type	*Installed with virus definitions?	64-bit package (MB)	32-bit package (MB)
Standard and Embedded CoreDefs-3**	Yes	188	175
	No	93	81
Dark network CoreDefs-1.5	Yes	288	276
	No	93	80

#### Choosing whether to download cloud-based or local-based definitions using the client installation type

For these packages, you can set a larger heartbeat. These sizes do not include packet-level firewall logs, which are not recommended in a production environment. If client logging is disabled, and there are no new policies or content to download from the management server, the client installation package is smaller. In this case, you can set a smaller heartbeat.

\* If your network has low bandwidth, install the client package without the virus definitions. As soon as the client connects to the management server, the client receives the full set of virus definitions.



---

All client installation packages include all features, such as Virus and Spyware, the firewall, the IPS, SONAR, System Lockdown, Application Control, Host Integrity content, and so forth. The difference between the client types are the size of the virus and spyware definitions.

Content updates require less storage space in the database and on the file system. Instead of storing multiple full revisions, the management server now stores only one full content revision plus incremental deltas. Full content updates require ~470 MB.

#### NOTE

You can download security patches to clients the same way as other content, using a LiveUpdate server, the management server, or a Group Update Provider. [Downloading Endpoint Protection security patches to Windows clients](#)

## Creating custom Windows client installation packages in Symantec Endpoint Protection Manager

You can customize client installation packages for Symantec Endpoint Protection for Windows by configuring the client installation settings and the client feature sets. This customization lets you configure an installation path, the restart behavior after installation, whether the installation package uninstalls a third-party security product, among others.

#### NOTE

Client Install Settings and Client Install Feature Set configurations only apply to Windows install packages. You can export a Macintosh or Linux install package through **Admin > Install Packages > Client Install Package**, but the configuration options differ.

**Table 37: Tasks to create a custom Windows client installation package**

Task	Details
Create a new custom client installation settings configuration	Use <b>Client Install Settings</b> to define the installation behavior. If you want to uninstall existing security software on your client computers, you configure it here. <a href="#">Customizing the client installation settings</a> <a href="#">Configuring client packages to uninstall existing security software</a>
Create a new custom feature set	<b>Client Install Feature Sets</b> define what protection technologies install on the client computer. <a href="#">Choosing which security features to install on the client</a>
Create a new, custom installation package	When you export a client installation package, you select from the customized settings files you created. You also choose to where you save the package, and whether the package is a single file (.EXE) or a folder of files. You can also use the custom installation settings and the custom feature sets with the Client Deployment Wizard. <a href="#">Exporting client installation packages</a> <a href="#">Installing Symantec Endpoint Protection clients with Remote Push</a>

[Preparing for client installation](#)

## About the Windows client installation settings

The Client Deployment Wizard prompts you to specify the client installation settings for Windows clients. The client installation settings define the options of the installation process itself. You can define the target installation folder, whether to disable installation logging, and the post-installation restart settings, among other options.

---

You can choose the default client installation settings, or you can add a custom **Client Install Settings** under **Admin > Install Packages > Client Install Settings**. The contextual Help provides details about the settings that you can configure.

You should use silent installations for remote deployment to minimize user disruption. When you use a silent deployment, you must restart the applications that plug into Symantec Endpoint Protection, such as Microsoft Outlook.

If you use unattended installations (**Show progress bar only**), Windows may display to users one or more pop-up windows. However, the installation should not fail even if the user does not notice them.

You should not use an interactive installation for remote deployment. This installation type fails unless the user interacts with it. Security features (such as Windows Session 0 isolation) on some operating systems may cause the interactive installation wizard to not appear. You should only use the interactive installation type for local installations. These recommendations apply to both 32- and 64-bit operating systems.

[Customizing the client installation settings](#)

[Choosing which security features to install on the client](#)

## Customizing the client installation settings

You can change the installation settings that you apply to a client installation package and for AutoUpgrade.

For example, if you want to install the client to a custom installation folder, or reset the client-server communication settings, you create custom client installation settings. You then apply this custom setting when you export or deploy a package, or set up AutoUpgrade.

To customize the client installation settings

1. In the console, click **Admin > Install Packages > Client Install Settings**.

2. Under **Tasks**, click **Add Client Install Settings**.

The default client install settings files cannot be modified.

3. Choose the operating system for which the setting file applies.

4. Enter a name and a description.

5. Make your selections from the available options on these tabs:

- Windows: **Basic Settings** and **Restart Settings**
- Mac: **Restart Settings** and **Upgrade Settings**

Mac client restart and upgrade settings apply only to AutoUpgrade (Version 14 and later).

6. Click **OK**.

When you run the Client Deployment Wizard or configure AutoUpgrade, select the settings that you created from the drop-down menu next to **Install Settings**.

[About the Windows client installation settings](#)

[Configuring client packages to uninstall existing security software](#)

## Uninstalling existing security software

You can configure and deploy new installation packages to uninstall existing security software before the installation of the Symantec Endpoint Protection client. Uninstalling existing security software allows the Symantec Endpoint Protection client to run more efficiently. You can remove existing third-party security software or an existing Symantec Endpoint Protection client.

---

You enable the security software removal feature by creating or modifying a custom client installation settings configuration. You then select this custom configuration during deployment.

You can use this feature to uninstall third-party security software. To see which third-party software the client package removes, see: [Third-party security software removal in Endpoint Protection 14](#). Some programs may have special uninstallation routines, or may need to have a self-protection component disabled. See the documentation for the third-party software.

You cannot remove third-party security software with Mac or Linux client packages. You must uninstall third-party security software before you deploy the Symantec Endpoint Protection client package.

#### NOTE

Changes to the third-party security software removal for version 14.2 means that you cannot enable it for installation packages for earlier versions. For example, you cannot enable third-party security software removal for version 14.0.1 client packages if you create them with and deploy them from Symantec Endpoint Protection Manager version 14.2.

In 14 and later, you can also remove existing installations of Symantec Endpoint Protection that you cannot uninstall through standard methods, such as Windows Control Panel. This feature appears as a separate option in the client installation settings.

Only the packages you create using the following procedure can remove existing security software.

1. To configure client packages to uninstall existing security software, in the console, on the **Admin** page, click **Install Packages**, and then click **Client Install Settings**.
2. Under **Tasks**, click **Add Client Install Settings**.

#### NOTE

If you have previously created a custom client installation settings configuration, you can modify it under **Tasks**, and then click **Edit Client Install Settings**. Modifying an existing custom configuration does not modify previously exported install packages.

3. On the **Basic Settings** tab, click one of the following options:
  - **Automatically uninstall existing third-party security software**
  - To remove a corrupted version of the Symantec Endpoint Protection client, use **Remove existing Symantec Endpoint Protection client software that cannot be uninstalled** (14)  
[About uninstalling the Symantec Endpoint Protection client](#)
4. Read the information about the option you chose, and then click **OK**.

You can also modify other options for this configuration. Click **Help** for more information about these options.
5. Click **OK** to save the configuration.
6. To deploy client packages to uninstall existing security software, in the console, on the **Home** page, launch the **Client Deployment Wizard**.

Click **Help > Getting Started Page** and then under **Required tasks**, click **Install the client software on your computers**.
7. In the **Client Deployment Wizard**, click **New Package Deployment**, and then click **Next**.

You can use **Existing Package Deployment** to deploy install packages you previously created. However, you must have exported these packages using a custom client installation settings configuration like the one described in the previous procedure.

8. In **Select Group and Install Feature Set**, select a Windows install package. In the **Install Settings** drop-down list, select the custom client installation settings configuration that you created or modified in the previous procedure. Click **Next**.
9. Click the deployment method that you want to use, and then click **Next** to proceed with and complete your chosen deployment method.

[Choosing a method to install the client using the Client Deployment Wizard](#)

[About the Windows client installation settings](#)

[Preparing for client installation](#)

## Choosing whether to download cloud-based or local-based definitions using the client installation type

When you specify a Windows client installation package, you must choose whether to download definitions from the cloud or locally. The cloud-enabled options include a standard client and an embedded/VDI client. Symantec Endpoint Protection also includes a dark network installation for clients that are not connected to the cloud.

### NOTE

If you want to change between the Windows client installation types: **Standard client**, **Embedded or VDI**, **Dark network**, at a later time after client installation, you **must** first uninstall the existing client software, reconfigure these settings, and then reinstall the new client package.

Standard client	Dark network client	Embedded/VDI client
<ul style="list-style-type: none"><li>• Uses virus and spyware definitions in the cloud.</li><li>• Installs only the latest virus and spyware definitions on disk. The standard client is approximately 80 percent to 90 percent smaller on disk than legacy standard or dark network Windows clients.</li><li>• Handles AutoUpgrade with deltas rather than full installation.</li></ul>	<ul style="list-style-type: none"><li>• Cannot use definitions in the cloud.</li><li>• Intended for clients with intermittent or no access to the cloud.</li><li>• Installs the full set of virus and spyware definitions.</li><li>• Similar to legacy standard-size client; uses reputation lookups for Download Insight and SONAR if connected to the cloud.</li><li>• Handles AutoUpgrade with deltas rather than full installation.</li></ul>	<ul style="list-style-type: none"><li>• Uses virus and spyware definitions in the cloud.</li><li>• Installs only the latest virus and spyware definitions. The client is approximately 80 percent to 90 percent smaller on disk than dark network Windows clients.</li><li>• The embedded/VDI client includes more size optimizations than the standard client:<ul style="list-style-type: none"><li>— The installer cache does not save after installation completes. This change means you cannot remove or modify the installation through the Control Panel unless you first copy the installation package to the client computer.</li><li>— The embedded client employs NTFS compression on more folders than the standard client.</li></ul></li><li>• Handles AutoUpgrade with full installation packages; cannot use deltas.</li></ul>

[Choosing a method to install the client using the Client Deployment Wizard](#)

[Exporting client installation packages](#)

---

## Third-party security software removal in Endpoint Protection 14

The following table lists the third-party security products that the Symantec Endpoint Protection client installation package can remove. The **Automatically uninstall existing third-party security software** option in the Client Install Settings dialog box removes these products.

Security products that are not in the supported products list can be removed using the [SEPprep tool](#).

**Table 38: List of third-party security products that the Client Installation Wizard removes**

Version	Third-party products
14.3 RU1	<a href="#">Third-party security software removal in Endpoint Protection 14.3 RU1</a>
14.3 MP1	<p>In 14.3 MP1 the <b>Automatically uninstall existing third-party security software</b> option was removed from the Symantec Endpoint Protection Manager. Instead, use the TPAR tool that is located in the Tools/TPAR folder of the Symantec Endpoint Protection download folder.</p> <p>The readme is located in: <a href="#">About the third-party security software removal feature in Symantec Endpoint Protection</a></p> <p>If you have a 14.3 MP1 Symantec Endpoint Protection Manager and you need to create an installation package for a 14.0 to 14.3 client, you can display and use the <b>Automatically uninstall existing third-party security software</b> option by adding <code>scm.uninstall.thirdparty.security.software.enabled=true</code> to the conf.properties file and then restarting the management server service.</p>
14.0 to 14.3	<a href="#">Third-party security software removal in Endpoint Protection 14</a>

[Uninstalling existing security software](#)

[About uninstalling the Symantec Endpoint Protection client](#)

## Third-party security software removal in Symantec Endpoint Protection 14.3 RU1 and later

The following table lists which third-party products and product versions that Symantec Endpoint Protection (SEP) can remove before the client installation package is installed. The client installation package removes any version of the product.

**Table 39: List of third-party security products that the 14.3 RU2 Client Installation Wizard removes**

Setting	Description
Avast	AntiVirus
AVG	AVG Internet Security Business Edition 2013
ESET	ESET Smart Security
Kaspersky	Kaspersky AntiVirus Kaspersky Endpoint Security Kaspersky Internet Security Kaspersky Security Center Network Agent
McAfee	McAfee Scan Enterprise

**Table 40: List of third-party security products that the 14.3 RU1 Client Installation Wizard removes**

Setting	Description
Avast	AntiVirus
AVG	AVG Protection
ESET	ESET Endpoint Antivirus / ESET Endpoint Security ESET Remote Administrator Agent
F-Secure	F-Secure Anti-Spyware F-Secure Anti-Spyware Scanner F-Secure Anti-Virus Client Security Installer F-Secure Automatic Update Agent F-Secure Backweb F-Secure Browsing Protection F-Secure CustomizationSetup F-Secure DAAS2 F-Secure Device Control F-Secure Diagnostics F-Secure E-mail Scanning F-Secure FWES F-Secure GateKeeper Interface F-Secure Gemini F-Secure GUI F-Secure Help F-Secure HIPS F-Secure Internet Shield F-Secure Localization API F-Secure Management Agent F-Secure Management Extensions F-Secure NAC Support F-Secure NAP Support F-Secure NIF F-Secure Offload Scanning Agent F-Secure ORSP Client F-Secure Policy Manager Support F-Secure Protocol Scanner F-Secure Safe Banking Popup F-Secure Sidegrade Support F-Secure Software Updater F-Secure System File Update F-Secure TNB F-Secure Uninstall F-Secure Anti-Virus
Kaspersky	Kaspersky Endpoint Security Kaspersky AES Encryption Module Kaspersky Anti-Virus for Windows Servers Kaspersky Security for Windows Servers Kaspersky Anti-Virus for Windows Workstations Kaspersky PURE Kaspersky Small Office Security Kaspersky AntiVirus / Kaspersky Internet Security Kaspersky Endpoint Security 8 for Windows Console Plug-in Kaspersky Anti-Virus SOS Kaspersky Security Center Network Agent

Setting	Description
McAfee	McAfee Endpoint Security Web Control McAfee Endpoint Security Firewall McAfee Endpoint Security Threat Prevention McAfee Endpoint Security Platform McAfee Desktop Firewall McAfee VirusScan Enterprise McAfee Firewall Protection Service McAfee Virus and Spyware Protection Service McAfee Browser Protection Service McAfee SiteAdvisor Enterprise McAfee Agent McAfee Product Improvement Program McAfee Host Intrusion Prevention
Sophos	Sophos Endpoint Agent Sophos Patch Agent Sophos Network Threat Protection Sophos System Protection Sophos Client Firewall Sophos Anti-Virus Sophos Exploit Prevention Sophos Remote Management System Sophos AutoUpdate Sophos Endpoint Defense
Trend Micro	Trend Micro OfficeScan Agent

With a 14.3 MP1 and later Symantec Endpoint Protection Manager (SEPM), you can no longer create an installation package that uses the **Automatically uninstall existing third-party security software** option in the Client Install Settings dialog box. Use TPAR instead. However, if you have a 14.3 MP1 SEPM and you're creating an installation package for a SEP client older than 14.3 MP1, you can use the feature, but you have to add **scm.uninstall.thirdparty.security.software.enabled=true** to conf.properties and then restart the management server services. This action unhides the checkbox. The option only works for clients versions 14.0 to 14.3, as they still contain the client-side feature.

## Restarting the client computers from Symantec Endpoint Protection Manager

You need to restart the Windows client computers after you install the client software. By default, the Windows client computers restart automatically after installation, though the user can delay it until a pre-scheduled time overnight. Before you export or deploy the installation package, you can configure the Windows client installation settings to customize the restart after installation. You can configure the restart options on a group to control how the client computers restart after a risk remediation or a new client download.

Mac client computers prompt for a restart after installation. If you push the client package and no one is logged on to the Mac computer, a hard restart occurs automatically when the installation completes. You cannot customize this setting.

Linux client computers do not require a restart and do not automatically restart after installation.

You can also restart the Mac and Windows client computers at any time by running a restart command from the management server. You cannot restart the Linux client with a restart command from the management server. You have the option to schedule the Windows client computers to restart during a time that is convenient for users. You can force

---

an immediate restart, or give the users an option to delay. When you send a restart command to a Mac client computer, it always performs a hard restart.

1. To configure risk remediation and new client download restart options on Windows client computers, in the console, click **Clients**.
2. On the **Clients** page, select a group, and then click **Policies**.
3. On the **Policies** tab, click **General Settings**.
4. In the **General Settings** dialog box, on the **Restart Settings** tab, select the restart method and schedule.

Some restart options apply only to Windows clients. For details, see the context-sensitive Help.

You can also add a notification that appears on the client computer before the restart occurs. The default message tells the user that a security risk remediation or a new content download requires a restart.

5. Click **OK**.
6. To restart a selected client computer, in the console, click **Clients**
7. On the **Clients** page, on the **Clients** tab, select a group.
8. On the **Clients** tab, select a client, right-click **Run command on computers**, and then click **Restart Client Computers**.
9. Click **Yes**, specify the restart options that you require, and then click **OK**.
10. To restart the client computers in a selected group, in the console, click **Clients**.
11. On the **Clients** page, on the **Clients** tab, select a group, click **Run a command on the group**, and then click **Restart Client Computers**.
12. Click **Yes**, specify the restart options that you require, and then click **OK**.

Some restart options apply only to Windows clients. For details, see the context-sensitive Help.

[About the Windows client installation settings](#)

[What are the commands that you can run on client computers?](#)

[Running commands on client computers from the console](#)

[Preparing for client installation](#)

## About managed and unmanaged clients

You can install the client software as a managed client or as an unmanaged client. In most cases, you should install a managed client. Install an unmanaged client so that the user has more control over the computer, such as a test computer, or if the computer is primarily off-site. Make sure that the unmanaged client users have the appropriate level of knowledge to configure any security settings that are different from the default settings.

You can convert an unmanaged client to a managed client at a later time by replacing the client-server communications file on the client computer.



**Table 41: Differences between a managed and an unmanaged client**

Type	Description
Managed client	<p>Managed clients connect to the Symantec Endpoint Protection Manager. You administer the client computers from the Symantec Endpoint Protection Manager console. You use the console to update the client software, security policies, and virus definitions on the managed client computers.</p> <p>The managed client can get content updates from Symantec Endpoint Protection Manager, GUPs, the Internet, and LiveUpdate.</p> <p>In most cases, you install the client software as a managed client.</p> <p><b>You can install a managed client in one of the following ways:</b></p> <ul style="list-style-type: none"><li>• During initial product installation</li><li>• From the console after installation</li></ul> <p>Version 14.0.1 or later cloud-managed features require a managed client.</p>
Unmanaged client	<p>The primary computer user must administer the client computer. An unmanaged client does not connect to Symantec Endpoint Protection Manager and cannot be administered from the console. In most cases, unmanaged clients connect to your network intermittently or not at all. The primary computer user must update the client software, security policies, and virus definitions on the unmanaged client computer.</p> <p>The unmanaged client can get content updates from the Internet and LiveUpdate. You must update the content on each client individually.</p> <p><a href="#">How to get an unmanaged client installation package</a></p> <p><a href="#">Installing an unmanaged Windows client</a></p>

[How does the client computer and the management server communicate?](#)

[How do I replace the client-server communications file on the client computer?](#)

[Preparing for client installation](#)

## How to get an unmanaged client installation package

You can get the unmanaged Symantec Endpoint Protection client installation package in one of the following ways:

- Download a standalone client installer from the [Broadcom Support Portal](#).
- Copy a folder from within the full installation file from the [Broadcom Support Portal](#).
- Export an unmanaged client from Symantec Endpoint Protection Manager with the default policies and settings, or with custom policies and settings.

### NOTE

For guidance in downloading the software, see: [Download the latest version of Symantec Endpoint Protection](#)

### To download the standalone client installer:

1. Sign in to the [Broadcom Support Portal](#).
2. Download the following file:  
Symantec\_Endpoint\_Protection\_version\_All\_Clients\_lang.zip  
Where version is the version number, and lang is the language, such as EN for English.
3. Extract the contents of the file to your hard drive.
4. Depending on the operating system on which you want to install the client, do one of the following:
  - For Windows: Copy the 32-bit or 64-bit .exe file to the target computer.
  - For Mac: Copy the Mac client .zip file to the target computer.
  - For Linux: Copy the Linux client .zip file to the target computer.

---

## NOTE

Symantec Agent or Symantec Endpoint Protection for Linux 14.3 RU1 and later cannot run as an unmanaged client.

### To copy the folder from the full installation file:

1. Sign in to the [Broadcom Support Portal](#).
2. Download the following file:  
Symantec\_Endpoint\_Protection\_version\_Full\_Installation\_lang.exe  
Where version is the version number, and lang is the language.
3. Double-click on the file to extract its contents.
4. Do one of the following:
  - For versions 14.2 MP1a (14.2.1023.0100) or later, the file extracts to C:\Users\username\AppData\Local\Temp\7zXXXXXXXXXX, where XXXXXXXXXX represents a random string of letters and numbers. Navigate to that folder. Do not close the installation menu.
  - For versions earlier than 14.2 MP1a (14.2.1023.0100), type or browse to a folder to extract to, and then click **Extract**. When the extraction finishes, navigate to that folder.
5. Depending on the operating system on which you want to install the client, do one of the following:
  - For Windows: Copy the folder **SEP** (32-bit) or **SEPx64** (64-bit) to the target computer.
  - For Mac: Copy the folder **SEP\_MAC** to the target computer.
  - For Linux: Copy the folder **SEP\_LINUX** to the target computer.

### To export an unmanaged client from Symantec Endpoint Protection Manager:

1. Log on to Symantec Endpoint Protection Manager.
2. Do one of the following:
  - Export an unmanaged client from Symantec Endpoint Protection Manager with the default policies and settings.  
[Exporting client installation packages](#)
  - Export an unmanaged client from Symantec Endpoint Protection Manager with custom policies and settings. For recommendations, see:  
[Recommended policies and settings for unmanaged client installation packages](#)  
You cannot export an unmanaged Mac client with group policies.  
You can then install the unmanaged client for Windows, Mac, or Linux.  
If the file is a .zip file, you must extract all contents before you install.

[Installing an unmanaged Windows client](#)

[About managed and unmanaged clients](#)

## Installing an unmanaged Windows client

An unmanaged (or self-managed) client usually allows a user greater control of Symantec Endpoint Protection settings through the client user interface. Typically, you install an unmanaged Symantec Endpoint Protection client directly on to a Windows computer, and the installation requires user input to complete.

[About managed and unmanaged clients](#)

[How to get an unmanaged client installation package](#)

## NOTE

When you install a managed Windows client installation package directly on to the client computer, the steps to install are similar. Only an **Interactive** installation requires user input. The client installation setting options **Show progress bar only** and **Silent** do not require user input.

---

## NOTE

Unmanaged client packages that are configured with custom policies may not display during installation some of the panels that are described. If you do not see an installation panel that the procedure step describes, skip to the next step.

1. Double-click `Setup.exe`, and then click **Next**.
2. On the **License Agreement Panel**, click **I accept the terms in the license agreement**, and then click **Next**.
3. On the **Setup Type** panel, click one of the following options:
  - Click **Typical** for the most common options, and then click **Next**.
  - Click **Custom** to configure your installation, and then click **Next**.
    - On the **Installation Type** panel, choose whether to download definitions from the cloud or locally (dark network).
    - On the **Custom Setup** panel, choose which features you want to install on the computer. A red X on a feature does not install.

[Choosing which security features to install on the client](#)

[Choosing which security features to install on the client](#)

4. If the installation wizard prompts you, click **Enable Auto-Protect** and **Run LiveUpdate**, and then click **Next**.
5. On the **File Reputation Data Submission** and **Data Collection** panels, uncheck the box if you do not want to provide pseudonymous data to Symantec, and then click **Install**.

An unmanaged client does not submit the data without a paid license, even if you leave the box checked.
6. On the **Wizard Complete** panel, click **Finish**.

[About the Windows client installation settings](#)

[Preparing for client installation](#)

## About uninstalling the Symantec Endpoint Protection client

You can uninstall the existing client installation on the client computer before the installation of Symantec Endpoint Protection begins. This feature is comparable to the CleanWipe utility, so you should not enable it for all deployments. Instead, you should only use this feature to remove corrupted or malfunctioning installations of the Symantec Endpoint Protection client.

Before you use the **Remove existing Symantec Endpoint Protection client software that cannot be uninstalled** feature, be aware of this important information:

- This feature can remove all Symantec Endpoint Protection versions up to and including the version of the installation package you create.
- This feature cannot uninstall a version of Symantec Endpoint Protection that is later than the installation package with which you include it. For example, you cannot use this feature during a planned rollback.
- If you deploy the wrong package type with this feature enabled, it does not perform the removal. For example, if you deploy a 32-bit package to a 64-bit computer, it cannot install. Therefore, it does not remove the existing Symantec Endpoint Protection installation.
- You cannot use this feature with an installation that uses the .MSI file directly, such as through a GPO deployment.
- This feature does not work with a manual upgrade or AutoUpgrade. You use this feature with a fresh installation only.
- This feature does not remove Symantec Endpoint Protection Manager.
- This option only removes Windows LiveUpdate if no other Symantec products use it.
- On the client computer, this feature runs silently, and does not display a status screen or user interface.
- This option forces the installation type to **Silent**.
- The computer restarts automatically after the removal completes. You cannot configure this restart to be postponed or skipped.

[Configuring client packages to uninstall existing security software](#)

## Uninstalling the Symantec Endpoint Protection client for Windows

You can uninstall the Windows client in the following ways:

- By using the Windows Control Panel to remove an application, typically **Programs and Features**.
- By configuring and deploying a custom client installation package that removes the Symantec Endpoint Protection client (as of 14). Only use this method if uninstalling with the Windows Control Panel does not work.  
[About the Symantec Endpoint Protection client preinstall removal feature](#)
- For alternative methods to uninstall Symantec Endpoint Protection Manager and other components, see [Uninstall Symantec Endpoint Protection](#).

If the Symantec Endpoint Protection client software uses a policy that blocks hardware devices, the policy blocks the devices after you uninstall the software. If you do not disable the device control by policy before you uninstall, use the Windows Device Manager to unblock the devices.

To uninstall the Symantec Endpoint Protection client for Windows

1. In the console, on the **Admin** page, click **Install Packages**, and then click **Client Install Settings**.
2. Under **Tasks**, click **Add Client Install Settings**.

### NOTE

If you have previously created a custom client installation settings configuration, you can modify it under **Tasks**, and then click **Edit Client Install Settings**. Modifying an existing custom configuration does not modify previously exported install packages.

3. On the **Basic Settings** tab, check **Remove existing Symantec Endpoint Protection client software that cannot be uninstalled**.
4. Read the message, and then click **OK**.
5. Click **OK**.

[Uninstalling the Symantec Endpoint Protection client for Mac](#)

[Uninstalling the Symantec Endpoint Protection client for Linux](#)

## Uninstalling the Symantec Endpoint Protection client for Mac

You uninstall the Symantec Endpoint Protection client for Mac through the client icon on the menu bar. Uninstallation of the Symantec Endpoint Protection client for Mac requires administrative user credentials.

### NOTE

After you uninstall the Symantec Endpoint Protection client, you are prompted to restart the client computer to complete the uninstallation. Make sure that you save any unfinished work or close all open applications before you begin.

---

### To uninstall the Symantec Endpoint Protection client for Mac:

1. On the Mac client computer, open the Symantec Endpoint Protection client, and then click **Symantec Endpoint Protection > Uninstall Symantec Endpoint Protection**.
2. Click **Uninstall** again to begin the uninstallation.
3. To install a helper tool that is needed for uninstalling the Symantec Endpoint Protection client, enter your Mac's administrative username and password, and then click **Install Helper**.
4. In the **Symantec Endpoint Protection is trying to modify a System Extension** dialog box, enter your Mac's administrative username and password, and then click **OK**.

You may also be prompted to type a password to uninstall the client. This password may be a different password than your Mac's administrative password.

5. Once the uninstallation completes, click **Restart Now**.

If the uninstallation fails, you may have to use an alternate method to uninstall. See:

[Uninstall Symantec Endpoint Protection](#)

## Uninstalling the Symantec Agent for Linux or the Symantec Endpoint Protection client for Linux

You uninstall the Symantec Endpoint Protection client for Linux with the script that the installation provides.

### NOTE

You must have superuser privileges to uninstall the Symantec Endpoint Protection client on the Linux computer. The procedure uses `sudo` to demonstrate this elevation of privilege.

### (For 14.3 RU1 and later) To uninstall the Symantec Management Agent for Linux:

1. On the Linux computer, open a terminal application window.
2. Navigate to the following directory:  
`/usr/lib/symantec/`
3. Run the following built-in script to uninstall Symantec Agent for Linux:  
`./uninstall.sh`
4. Reboot the computer after the uninstallation finishes and the reboot prompt appears.  
Note that the `uninstall.sh` script will remove all components of Symantec Agent for Linux (`sdcss-caf`, `sdcss-sepagent`, and `sdcss-kmod`).  

```
[root@localhost symantec]# ./uninstall.sh
Running ./uninstall.sh (PWD /usr/lib/symantec; version 2.2.4.41)
Uninstalling Symantec Agent for Linux (SEPM) ...
Removing packages sdcss-caf sdcss-sepagent sdcss-kmod sdcss-scripts
Symantec Agent for Linux (SEPM) uninstalled successfully.
A reboot is required to complete uninstallation.
Please reboot your machine at the earliest convenience.
```

### (For 14.3 MP1 and earlier) To uninstall the Symantec Endpoint Protection client for Linux:

1. On the Linux computer, open a terminal application window.
2. Navigate to the Symantec Endpoint Protection installation folder with the following command:  
`cd /opt/Symantec/symantec_antivirus`  
The path is the default installation path.

- 
3. Use the built-in script to uninstall Symantec Endpoint Protection with the following command:

```
sudo ./uninstall.sh
```

Enter your password if prompted.

This script initiates the uninstallation of the Symantec Endpoint Protection components.

4. At the prompt, type **Y** and then press **Enter**.

Uninstallation completes when the command prompt returns.

**NOTE**

On some operating systems, if the only contents of the `/opt` folder are the Symantec Endpoint Protection client files, the uninstaller script also deletes `/opt`. To recreate this folder, enter the following command:

```
sudo mkdir /opt
```

To uninstall using a package manager or software manager, see the documentation specific to your Linux distribution.

---

# Upgrading and Migrating to the Latest Release of Symantec Endpoint Protection (SEP)

---

Learn how to update to the latest release of Symantec Endpoint Protection

Use this topic to upgrade to the latest release of SEP 14.x and take advantage of the new features. This information is specific to upgrading the software in environments where a compatible version of the product is already installed.

Before you upgrade, review the following information:

- [Release notes, new fixes, and system requirements for all versions of Endpoint Protection](#)
- [Known issues and workarounds](#)
- [What's new for all releases of Symantec Endpoint Protection 14.x](#)
- [Supported and unsupported upgrade paths to the latest version of Symantec Endpoint Protection 14.x](#)
- [Symantec Endpoint Protection 14 Migration Considerations](#)

**Table 42: Process for upgrading Symantec Endpoint Protection**

Task	Description
Step 1: Download the latest version from the Broadcom Download Center	<a href="#">Download the latest version of Symantec software</a> Before you upgrade the Symantec Endpoint Protection Manager (SEPM) and the Symantec Endpoint Protection clients, make sure you maximize the protection of your network during the upgrade by following these best practices: <ul style="list-style-type: none"><li>• Symantec recommends that you do not perform third-party installations simultaneous to the upgrade of Symantec Endpoint Protection. Installing third-party software that makes network- or system-level changes may cause undesirable results when you upgrade Symantec Endpoint Protection.</li><li>• If possible, restart client computers before installing or upgrading Symantec Endpoint Protection.</li><li>• Symantec recommends that you upgrade the entire network to the current version of Symantec Endpoint Protection, rather than manage multiple versions.</li></ul> <a href="#">Upgrade best practices for Endpoint Protection 14.x</a>
Step 2: Back up the database and prepare for disaster recovery	Back up the database, logs, and recovery file that Symantec Endpoint Protection Manager uses to ensure the integrity of your client data. These steps are different depending on your version. <a href="#">Disaster recovery best practices for Endpoint Protection</a>
Step 3: Break the replication relationship	If the management server you want to update replicates with other management servers, break the replication relationship. If the replication partner launches replication during the upgrade, it may have unpredictable results.  <b>Note:</b> Breaking the relationship between the management servers is not the same as removing the replication partner. You do not want to delete the replication partner entirely.  If you do not use replication between management servers, you can skip this step.

Task	Description
Step 3: Stop the Symantec Endpoint Protection Manager service	<p>You must manually stop the management server service on all sites before you install a newer version. The management server service stops the Syslog service or similar service that runs on the SEPM and which could potentially lock SEPM files or folders and cause the upgrade to fail. After you upgrade, the management server automatically starts the service.</p> <p>If the management server replicates with other management servers, make sure that replication does not occur during the period that you upgrade the SEPM and that the management server service is stopped.</p> <p><b>Note:</b> <a href="#">Preventing replication during an upgrade</a></p>
Step 4: Upgrade the Symantec Endpoint Protection Manager software	<p>Install the new version of Symantec Endpoint Protection Manager over the existing version on all sites in your network. The existing version is detected automatically, and all settings are saved during the upgrade.</p> <p><a href="#">Upgrading a management server</a></p> <p><a href="#">Installing Symantec Endpoint Protection Manager</a></p> <p>If you enrolled a Symantec Endpoint Protection Manager domain into the ICDm cloud console (hybrid management) before the upgrade, the domain remains enrolled during the upgrade process. You can also enroll any domain after the upgrade.</p> <p><a href="#">Enrolling a domain in the cloud console from the Symantec Endpoint Protection Manager</a></p>
Step 5: Restore the replication relationship after upgrade	<p>If the management server you updated replicates with other management servers, restore the replication relationship.</p> <p>If you do not use replication between management servers, you can skip this step.</p> <p><a href="#">Disabling replication and restoring replication before and after an upgrade</a></p>
Step 5: Upgrade Symantec client software	<p>You do not need to uninstall previous clients before you install the new version. The over install process saves the client settings, and then upgrades the client to the latest version. You should first update a group with a small number of test computers before you update your entire production network.</p> <p>If you use clients as Group Update Providers, you must upgrade them first. <a href="#">Upgrading Group Update Providers</a></p> <p>Review the applicable steps in <a href="#">Preparing for client installation</a> and <a href="#">Preparing Windows and Mac computers for remote deployment</a>. Then choose from one of the available methods to upgrade clients:</p> <ul style="list-style-type: none"> <li> <b>AutoUpgrade:</b> AutoUpgrade is the easiest way to update the Windows and Mac client software in groups.  You assign client packages to groups in the management server, either manually or by using the <b>Upgrade Clients with Package</b> wizard. No further action is required on your part to complete the upgrade process.  <a href="#">Upgrading client software with AutoUpgrade</a>  <b>AutoUpgrade</b> does not support the Symantec Agent for Linux 14.3 RU1. </li> <li> <b>Installation file:</b> Download the client installation file from the <a href="#">Broadcom Download Center</a>.  <a href="#">Download the latest version of Symantec software</a> </li> <li> <b>Client Deployment Wizard:</b> Run the Client Deployment wizard in the management server. This wizard walks you through the creation of a client package that can be deployed by a web link and email, remote push, or saved for a later local installation. You can also deploy using third-party tools.  <a href="#">Choosing a method to install the client using the Client Deployment Wizard</a> </li> </ul>

## Upgrade best practices for Endpoint Protection 14.x

The following resources help you to plan and perform an optimal upgrade to the current version of Symantec Endpoint Protection (SEP). Follow the recommended best practices and be aware of any potential issues and risks.



- [Benefits of upgrading to the latest version](#)
- [Important information for the latest version](#)
- [Things to know before getting started](#)
- [Best practices](#)
- [Frequently asked questions \(FAQ\)](#)

### Benefits of upgrading to the latest version

To get the latest security features, operating system support, and customer fixes, upgrade to the latest version. For information on what features each version offers, see:

[What's new for all releases of Symantec Endpoint Protection \(SEP\) 14.x](#)

### Important information for the latest version

System requirements and release notes	<p>Review carefully before you upgrade:</p> <p><a href="#">Release notes, new fixes, and system requirements for all versions of Endpoint Protection</a></p> <p>Before the upgrade, use the <a href="#">Symantec Diagnostic tool</a> to determine whether the computers meet minimum system requirements.</p> <p>If you plan to upgrade your operating system, be sure to first upgrade Symantec Endpoint Protection to a version that supports the operating system. Leaving an unsupported version of Symantec Endpoint Protection in place when you upgrade the operating system can have unexpected results.</p>
Supported and unsupported upgrade paths	<p>Make sure that the currently installed version can be migrated or upgraded to the new version. Review the following articles:</p> <p><a href="#">Symantec Endpoint Protection Migration Considerations</a></p> <p><a href="#">Supported and unsupported upgrade paths to the latest version of Symantec Endpoint Protection 14.x</a></p>
Important installation and upgrade information	<ul style="list-style-type: none"> <li>• Symantec Endpoint Protection 14.3 RU2 clients cannot be managed by a 14.3 RU1 MP1 or earlier Symantec Endpoint Protection Manager.</li> <li>• For an upgrade to 14.3 RU1 or later, the default Microsoft SQL Server Express database replaces the embedded database. The maximum database size is 10 GB.</li> <li>• For an upgrade to 14.2 or later, firewall policies cannot incorporate the changes for IPv6 if some default names have been changed. The default names include the names of default policies and default rule names. If the rules cannot be updated during the upgrade, the IPv6 options do not appear. Any new policies or rules that you create after the upgrade are not affected.</li> </ul> <p>If possible, revert any changed names back to the default. Otherwise, ensure that any custom rules that you added to a default policy do not block IPv6 communication in any way. Ensure the same for any new policies or rules that you add.</p> <p>These actions prevent any issues with IPv6 communications.</p> <ul style="list-style-type: none"> <li>• You cannot upgrade legacy Symantec Endpoint Protection clients to version 14.2 or later if the network only uses IPv6 communications. In this context, legacy clients are Symantec Endpoint Protection clients with a version earlier than 14.2. These earlier client versions do not support IPv6 communication, so the upgrade can result in communication issues with Symantec Endpoint Protection Manager.</li> </ul> <p>Upgrade the clients to version 14.2 before moving the environments to a pure IPv6 network. Alternately, uninstall the legacy versions, then deploy a new 14.2 or later package to these client computers.</p> <ul style="list-style-type: none"> <li>• If Symantec Endpoint Protection uses a SQL Server database and your environment only uses TLS 1.2, ensure that SQL Server supports TLS 1.2. You may need to patch SQL Server. See: <a href="#">TLS 1.2 support for Microsoft SQL Server</a></li> </ul> <p>This recommendation applies to SQL Server 2008, 2012, and 2014.</p> <ul style="list-style-type: none"> <li>• New installations of Symantec Endpoint Protection Manager enable secure communications between the clients and the management console. The upgrade maintains current communication configuration.</li> </ul>

### Things to know before you get started

The following table lists the recommended routine maintenance tasks you should perform before you upgrade. Maintenance may include disk error checks, defragmentation of the hard drive, or other routine health checks.

Insufficient disk space	Ensure that the management server has enough disk space to perform the upgrade. For a successful Symantec Endpoint Protection Manager upgrade, free space should be at least three times the size of the database. Consult the system requirements for the free space that is required to install the Symantec Endpoint Protection client. <a href="#">Increasing Symantec Endpoint Protection Manager available disk space before an upgrade.</a>
Proxy servers	Ensure that you have made the proper exclusions to any peripheral firewall or proxy to ensure successful communication with all Symantec servers. <a href="#">URLs that allow SEP and SES to connect to Symantec servers</a>
Scanning exclusions	You may need to create additional scanning exclusions before you deploy the client upgrade. See: <ul style="list-style-type: none"> <li>• <a href="#">What scan exclusions should be applied to all Windows clustered server nodes?</a></li> <li>• <a href="#">About the automatic exclusion of files and folders for Microsoft Exchange server and Symantec products</a></li> <li>• <a href="#">Best practices for virtualization</a></li> <li>• <a href="#">Excluding known risks from virus and spyware scans on Windows clients</a></li> </ul>
Steps to upgrade	For general information on upgrading Symantec Endpoint Protection, see <a href="#">Upgrading and Migrating to the Latest Release of Symantec Endpoint Protection (SEP)</a> .
Upgrading unsupported languages	As of 14.3 RU2, both the Symantec Endpoint Protection Manager (SEPM) and the clients are translated into five languages only: English, Brazilian Portuguese, French, Japanese, and Spanish. When you upgrade the SEPM from a non-supported language, SEPM automatically upgrades to English. If you want to upgrade to a different supported language, such as from Czech to French, before you upgrade, see: <a href="#">Upgrading Symantec Endpoint Protection Manager 14.3 RU2+ to a supported language</a> To upgrade an unsupported language on the Windows client, see: <a href="#">Upgrading client software with AutoUpgrade</a>

## Best practices

Back up before you upgrade	As a best practice, always back up the Symantec Endpoint Protection Manager database before an upgrade. <a href="#">Backing up the database and logs</a>
AutoUpgrade	Use the <b>Upgrade Clients with Package</b> wizard to upgrade existing Windows and Mac clients. You may want to schedule AutoUpgrade for after hours, due to possible bandwidth usage. You can stage client packages on a web server, and then run <b>Upgrade Clients with Package</b> . There are alternate methods to deploy the upgrade package as well, such as through the Client Deployment Wizard. <a href="#">Upgrading client software with AutoUpgrade</a>
Fresh install of Symantec Endpoint Protection Manager	You can use the Communication Update Package to connect existing clients to a new installation of the Symantec Endpoint Protection Manager. For example, if you decommission an existing server, and install Symantec Endpoint Protection Manager to a new server instead. Create a new client installation setting that resets client-server communications settings, and then deploy the Communication Update Package in the same way as clients: <b>Help &gt; Getting Started Page &gt; Install the client software on your computers</b> . You can also reset the client-server communications settings for Mac computers with a client installation setting. After the clients are connected, you can upgrade the clients with AutoUpgrade. <a href="#">About the Windows client installation settings</a>

Virtualization	<p>The Symantec Endpoint Protection clients can be used to protect virtual instances of the supported operating systems.</p> <p>Symantec Endpoint Protection Manager can be installed and managed on virtual instances of the supported operating systems. Symantec Endpoint Protection includes additional management options for virtual clients, such as Shared Insight Cache and a separate configuration option for purging offline non-persistent GVMs.</p> <p><a href="#">Best practices for virtualization in Symantec Endpoint Protection</a></p>
Disaster recovery preparation	<p>Before you begin the upgrade, ensure that you have backed up the current Symantec Endpoint Protection Manager installation using disaster recovery preparation techniques. If the upgrade then fails, you can restore the Symantec Endpoint Protection Manager to functionality more quickly.</p> <p>To recover an installation after a failure, due to database schema and other changes, you must reinstall using the exact version previously in use.</p> <p>See <a href="#">Disaster recovery best practices for Endpoint Protection</a></p>

## Frequently asked questions (FAQs)

### Q: Where do I get the current version of Symantec Endpoint Protection?

A: From the Broadcom Support Portal. See the following page for guidance:

[Download the latest version of Symantec software](#)

Contact Technical Support for additional assistance: [Symantec Endpoint Security](#)

### Q: How do I activate my license?

A: After you log on to Symantec Endpoint Protection Manager, click **Help > Getting Started Page**, under **Required Tasks**.

### Q: What are the upgrade methods? When should each method be used?

A: There are many methods available to upgrade clients. Second, decide which method is most appropriate for the situation. Every situation is different, so Symantec provides many different methods for accomplishing this goal:

- AutoUpgrade: Assign client packages to groups in the management console, either manually or by using the **Upgrade Clients with Package** wizard.
- Local installation from the installation file or installation media.
- Run the Client Deployment Wizard from the management console. The Client Deployment Wizard walks you through the creation of a client package. You can then choose to deploy by emailing a web link to users, by a remote push. You can also save the package for local installation or with a third-party deployment tool.

Before you begin, ensure the client computers are ready to receive an upgrade package:

[Managing the Symantec Endpoint Protection client installation](#)

### Q: What's the recommended migration order? What do I upgrade first in my environment?

A: The recommended order is to upgrade is as follows:

1. Symantec Endpoint Protection Managers
2. Group Update Providers
3. The remaining clients as needed

### Q: Can I continue to manage Windows 2000 and Symantec Endpoint Protection 11.x clients?

A: No.

### Q: How can I generate a list of Symantec Endpoint Protection versions installed in my environment?

A: Generate this list using **Reports**.

[Generating a list of the Symantec Endpoint Protection versions installed in your network](#)

---

## Supported and unsupported upgrade paths to the latest version of Symantec Endpoint Protection 14.x

Generally, for Symantec Endpoint Protection versions earlier than the latest version, every version on the list before it is supported. However, you should confirm by referring to the release notes for your specific version.

[Release versions, notes, new fixes, and system requirements for Endpoint Security and all versions of Endpoint Protection](#)

### Supported upgrade paths

- Symantec Endpoint Protection Manager version 12.1.6 MP10 and later with the embedded database upgrades seamlessly to the Microsoft SQL Server Express database, version 14.3 RU1 MP1. Upgrades from 12.1.6 MP9 and earlier to 14.3 RU1 MP1 are blocked.
- Symantec Endpoint Protection Manager 14.x upgrades seamlessly over 12.1.x, except where support has been dropped, such as: Windows Server 2003, desktop operating systems, and 32-bit operating systems, as well as some versions of SQL Server.
- The Symantec Endpoint Protection 14.x client upgrades seamlessly over all previous 12.1 client versions installed on supported operating systems.

### [Symantec Endpoint Protection 14 Migration Considerations](#)

#### Symantec Endpoint Protection Manager and Windows client

The following versions of Symantec Endpoint Protection Manager and Symantec Endpoint Protection Windows client can upgrade directly to the current version:

- 11.x and Small Business Edition 12.0 (Symantec Endpoint Protection clients only, for supported operating systems)
- 12.1.x, up to 12.1.6 MP10
- 14, 14 MP1, 14 MP2
- 14 RU1, 14 RU1 MP1, 14 RU1 MP2
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1
- 14.3 RU1, 14.3 RU1 MP1, 14.3 RU2

#### Mac client

The following versions of Symantec Endpoint Protection client for Mac can upgrade directly to the current version:

- 12.1.4 - 12.1.6 MP9  
The Mac client did not update for version 12.1.6 MP10.
- 14, 14 MP1, 14 MP2
- 14 RU1, 14 RU1 MP1, 14 RU1 MP2  
The Symantec Endpoint Protection client for Mac was not updated for 14.0.1 MP2.
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1
- 14.3 RU1, 14.3 RU1 MP1 (available June 2021), 14.3 RU2

#### Linux client

---

**NOTE**

As of version 14.3 RU1, the Linux client installer detects and uninstalls the legacy Linux client (earlier than 14.3 RU1) and then performs a fresh install of the new client. Old configurations will not be retained.

The following versions of Symantec Endpoint Protection client for Linux can upgrade directly to current version:

- 12.1.x, up to 12.1.6 MP9  
The Linux client did not update for version 12.1.6 MP10.
- 14, 14 MP1, 14 MP2
- 14 RU1, 14 RU1 MP1, 14 RU1 MP2
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1
- 14.3 RU1, 14.3 RU1 MP1, 14.3 RU2

Symantec AntiVirus for Linux 1.0.14 is the only version that you can migrate directly to Symantec Endpoint Protection. You must first uninstall all other versions of Symantec AntiVirus for Linux. You cannot migrate a managed client to an unmanaged client.

**Unsupported upgrade paths**

You cannot migrate to Symantec Endpoint Protection from all Symantec products. You must uninstall the following products before you install the Symantec Endpoint Protection client.

- Symantec AntiVirus and Symantec Client Security, which are not supported.
- All Symantec Norton products
- Symantec Endpoint Protection for Windows XP Embedded 5.1
- Any Symantec Endpoint Protection for Mac client earlier than 12.1.4. Or you can upgrade it to 12.1.4 or later.

**Notes:**

- Any Symantec Endpoint Protection client migration for version earlier than 12.1.x is not supported.
- You cannot upgrade Symantec Endpoint Protection Manager 11.0.x or Symantec Endpoint Protection Manager Small Business Edition 12.0.x directly to any version of Symantec Endpoint Protection Manager 14. You must first uninstall these versions or perform an upgrade to 12.1.x before an upgrade to the latest release of 14.x.
- You cannot upgrade Symantec Endpoint Protection Manager 12.1.6 MP7 to version 14 because the database schema version in 12.1.6 MP7 is later than in 14. Instead, you must upgrade 12.1.6 MP7 to 14 MP1 or later.
- 14.0.x dropped support for Windows XP, Server 2003, and any Windows Embedded operating system that is based on Windows XP. Symantec Endpoint Protection Manager 14.2 RU1 can manage these computers as legacy 12.1.x clients, although 12.1.x clients are EOL. For these clients, you may want to use a Symantec product that still supports these legacy operating systems, such as Data Center Security (DCS).
- Upgrading from 14 MP1 (14.0.2332.0100) to 14 MP1 Refresh Build (14.0.2349.0100) is not supported.
- Downgrade paths are not supported. For example, if you want to migrate from Symantec Endpoint Protection 14.2.1.1 to 12.1.6 MP10, you must first uninstall Symantec Endpoint Protection 14.2.1.
- If you have a build number but you are not sure how it translates to release version, see:

[About Endpoint Protection release types and versions](#)

## Increasing Symantec Endpoint Protection Manager available disk space before an upgrade

The Symantec Endpoint Protection Manager installation requires a minimum amount of available disk space. Make sure that any current servers or new hardware meet the minimum hardware requirements. However, additional available disk space may be needed during an upgrade to allow for the creation of temporary files.

---

Make a backup of the database before making configuration changes.

### Backing up the database and logs

**Table 43: Tasks to increase disk space on the management server**

Task	Description
Change the LiveUpdate settings to reduce space requirements	<ol style="list-style-type: none"><li>1. Go to <b>Admin &gt; Servers</b> and right-click <b>Local Site</b>. Select <b>Edit Site Properties</b>.</li><li>2. On the <b>LiveUpdate</b> tab, reduce the number of content revisions to keep. For an upgrade, you can lower the setting to 10. Allow time for Symantec Endpoint Protection Manager to purge the extra revisions. However, the reduction of revision numbers may trigger full update downloads from the clients that check in. An increase in these full update requests may negatively affect network performance.</li></ol> <p><b>Note:</b> Returning the revision setting to its previous value after the upgrade completes is not necessary. Improvements to the way Symantec Endpoint Protection Manager stores and manages content means that a larger number of revisions takes up less disk space than in earlier versions.</p> <p><a href="#">How to update content and definitions on the clients</a> <a href="#">Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager</a></p>
Make sure that unused virus definitions are deleted from the Symantec Endpoint Protection Manager database	<ol style="list-style-type: none"><li>1. Go to <b>Admin &gt; Servers</b>, right-click the database server, and then select <b>Edit Database Properties</b>. The database name is <b>SQLEXPRESSSYM</b> (14.3 RU1 and later) or <b>localhost</b> (14.3 MPx and earlier). For a Microsoft SQL Server database, the database server name varies based on the location of your database.</li><li>2. On the <b>Log Settings</b> tab, under <b>Risk Log Settings</b>, make sure that <b>Delete unused virus definitions</b> is checked.</li></ol>
Relocate or remove co-existing programs and files	<ul style="list-style-type: none"><li>• If other programs are installed on the same computer with Symantec Endpoint Protection Manager, consider relocating them to another server. You can remove unused programs.</li><li>• If storage-intensive programs are installed on the same computer with Symantec Endpoint Protection Manager, consider dedicating a computer to support only Symantec Endpoint Protection Manager.</li><li>• Remove temporary Symantec Endpoint Protection Manager files. For a list of temporary files that you can remove, see the article, <a href="#">Symantec Endpoint Protection Manager directories contain many .TMP folders consuming large amounts of disk space</a>.</li></ul> <p><b>Note:</b> Defragment the hard drive after removing programs and files.</p>
Use an external database	<p>If the Symantec Endpoint Protection database resides on the same computer with Symantec Endpoint Protection Manager, consider installing a Microsoft SQL Server database on another computer. Significant disk space is saved and in most cases, performance is improved.</p> <p><a href="#">About choosing a database type</a></p>

#### NOTE

Make sure that the client computers also have enough disk space before an upgrade. Check the system requirements and as needed, remove unnecessary programs and files, and then defragment the client computer hard drive.

### Low disk space on a Symantec Endpoint Protection Manager

## Upgrading a management server

You must upgrade all management servers before you upgrade any clients.

If you upgrade management servers in an environment that supports load balancing, failover, or replication, you must prepare and upgrade them in a specific order.

---

## WARNING

You must follow the scenario that applies to your type of installation, or your upgrade can fail.

**Table 44: Upgrade tasks**

Task	Description
Upgrade the management server	<p>Review the system requirements and supported upgrade paths, upgrade the management server, and then configure it with the Management Server Configuration Wizard.</p> <p>As of 14, the following applies to a Symantec Endpoint Protection Manager upgrade:</p> <ul style="list-style-type: none"><li>Windows Server 2003, all desktop operating systems, and 32-bit operating systems are no longer supported.</li><li>SQL Server 2005 is no longer supported for the database. Support is also dropped for SQL Server 2008 earlier than SP4, and SQL Server 2008 R2 earlier than SP3.</li><li>You must now enter SQL Server system administrator credentials during the upgrade.</li></ul> <p><b>Note:</b> You may need to edit the domain security policies to allow the virtual service accounts to run correctly for Windows 7 / Server 2008 R2 or later.</p> <p><b>Note:</b> Error: "...services require user rights" or "...cannot read the user rights" during installation or configuration</p> <p><a href="#">Installing Symantec Endpoint Protection Manager</a></p> <p><a href="#">Supported upgrade paths to the latest version of Symantec Endpoint Protection 14.x</a></p>
Log onto the management server	<p>When the Symantec Endpoint Protection Manager logon panel appears, you can log on to the console by using your logon credentials.</p> <p><a href="#">Logging on to the Symantec Endpoint Protection Manager console</a></p>

## NOTE

You are not required to restart the computer after the upgrade, but you may notice performance improvements if you restart the computer and log on.

[Setting up failover and load balancing](#)

[Setting up sites and replication](#)

## Best practices for upgrading from the embedded database to the Microsoft SQL Server Express database

In 14.3 RU1, the default database that is installed with Symantec Endpoint Protection Manager (SEPM) changed from the embedded database to the Microsoft SQL Server Express 2017 database. When you upgrade or install the management server for the first time using the default configuration in the Management Server Configuration Wizard, the SQL Server Express database is installed automatically and replaces the embedded database.

When you upgrade to version 14.3 RU1 or later, the management server computer must fulfill certain requirements, or the management server upgrade cannot proceed. The Management Server Configuration wizard informs you if you encounter these issues and gives you the opportunity to fix them.

### Things to know before you upgrade



---

Before the upgrade, check the following issues that you may need to fix before you install.

Insufficient database size	<p>The SQL Server Express database has a maximum capacity of 10 GB for data files and log data. The Symantec Endpoint Protection Manager makes a backup of the embedded database before the installation starts. If that backup is larger than 10 GB, the upgrade cannot continue. You must reduce the amount of data either before you start the upgrade or during the upgrade. The Management Server Configuration wizard informs you when the database size is too large.</p> <p>If the database is over 10 GB before you start the installation, perform the following tasks:</p> <p><a href="#">Reducing the database size when the database is full before an upgrade to Microsoft SQL Server Express</a></p> <p>Both the Microsoft SQL Server Express database and the Microsoft SQL Server database use a feature called FILESTREAM to reduce the database size. If you find out that the database size is too large or close to too large during the upgrade, you can perform the following actions:</p> <p><a href="#">Enabling FILESTREAM for the Microsoft SQL Server database</a></p> <p><b>Note:</b> If you use the SQL Server database, periodically check the database size to make sure that the database does not reach its maximum size:</p> <p><a href="#">Increasing the Microsoft SQL Server database file size</a></p>
Insufficient disk space	<p>Ensure that there is a minimum of 10 GB of available disk space on the management server computer to perform the upgrade.</p> <p><a href="#">Making more disk space available to upgrade to the default Microsoft SQL Server Express database</a></p>
The Symantec Endpoint Protection Manager does not communicate with the database	<p>Symantec Endpoint Protection Manager uses a certificate to authenticate communications between the Symantec Endpoint Protection (SEPM) and the Microsoft SQL Server Express or SQL Server databases. You must generate the certificate and import it into the Symantec Endpoint Protection Manager computer for SEPM to connect to either the SQL Server database. If the certificate does not exist, is expired, or is about to expire, the connection between SEPM and the database fails.</p> <p><a href="#">Configuring encrypted communication between Symantec Endpoint Protection Manager and Microsoft SQL Server</a></p> <p>To check that the management server connects to the database, see:</p> <p><a href="#">Verifying the management server connection with the database</a></p>
Troubleshooting issues with upgrading to the Microsoft SQL Server Express	<p>You may have one of the following issues when you upgrade:</p> <ul style="list-style-type: none"><li>• The Windows update is out of date or the Windows update service is not running. To troubleshoot this issue, cancel the SEPM installation, run the latest update or restart the Windows update service, restart your computer, and then continue the Symantec Endpoint Protection Manager installation.</li><li>• The SQL Server Express database does not install. To troubleshoot, review the database logs. <a href="#">Troubleshooting Installation issues with the Endpoint Protection Manager's Default SQL Server Express database</a></li><li>• No connection between the Symantec Endpoint Protection Manager and the database. <a href="#">Verifying the management server connection with the database</a> <a href="#">Troubleshooting communication problems between Symantec Endpoint Protection Manager and the console or the default database</a></li><li>• You change the IP address and host name of the computer that Symantec Endpoint Protection Manager runs on <a href="#">Reconfiguring Symantec Endpoint Protection Manager after changing the computer's IP address and host name</a></li></ul>

[Backing up the database and logs](#)



---

## Reducing the database size when the database is full before an upgrade to Microsoft SQL Server Express

The default Microsoft SQL Server Express database has a size limit of 10 GB for data files and log data. When you upgrade from an embedded database with a size larger than 10 GB, and you are in the middle of the upgrade to Microsoft SQL Server Express, the upgrade process cannot continue.

If the Management Server Configuration Wizard detects that the database size is already too large, you may see the following messages:

The SQL Server Express database has reached its 10 GB limit. You must reconfigure the upgrade settings to import less data first. Then run the upgrade wizard again.

When the default database size is too large, pause the upgrade and perform the following steps:

### Step 1: : Decrease the number of days that logs are collected

In the following file, reduce the number of days: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\conf.properties

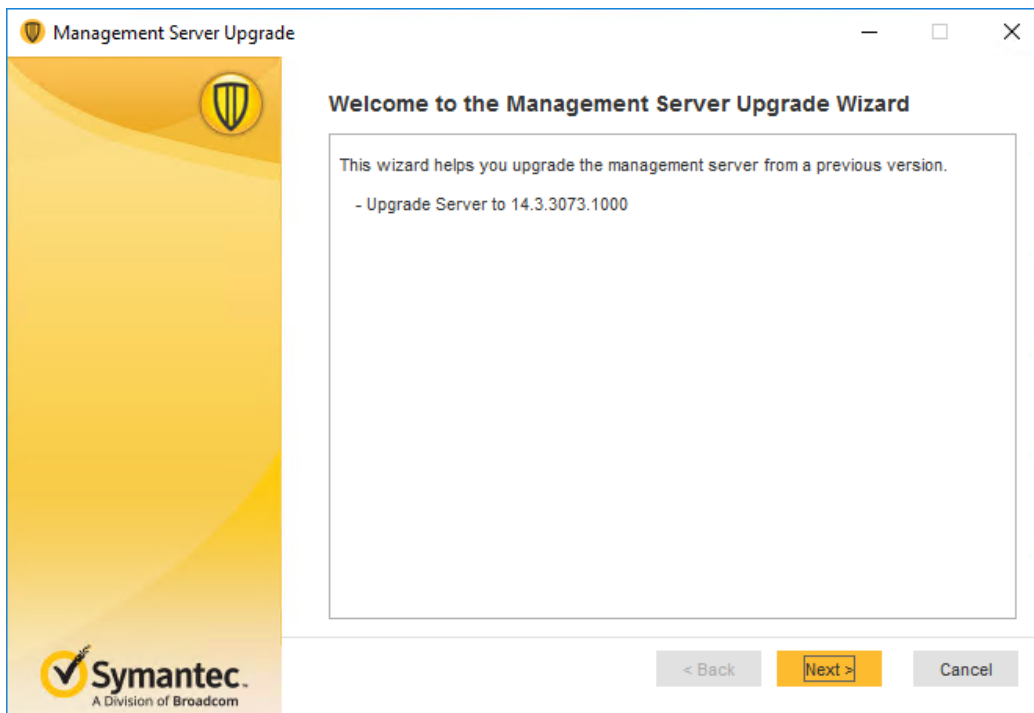
- scm.sqlexpress.migration.otherlog.days=7
- scm.sqlexpress.migration.learnedapps.days=0
- scm.sqlexpress.migration.clientserveractivity.days=3
- scm.sqlexpress.migration.traffic.days=7
- scm.sqlexpress.migration.packet.days=7
- scm.sqlexpress.migration.security.days=7

This reduces the amount of data that migrates to the SQL Server Express database.

**Note:** scm.sqlexpress.migration.clientserveractivity.days is already set to 7 by default to keep the database size smaller.

### Step 2: Restart the Management Server Upgrade Wizard

Double-click ..\Symantec\Symantec Endpoint Protection Manager\bin\upgrade.bat



#### NOTE

If you had started the **Database Backup and Restore** dialog box before you made these changes, restart it by double-clicking `..\Symantec\Symantec Endpoint Protection Manager\bin\dbtools.bat`

[Reducing the database size to less than 10 GB before an upgrade to Microsoft SQL Server Express](#)

## Enabling FILESTREAM for the Microsoft SQL Server database

This topic describes how to enable FILESTREAM for a Microsoft SQL Server database.

The Microsoft SQL Server database uses a feature called FILESTREAM to reduce the database size and to improve database performance.

- The Microsoft SQL Server Express database has a 10 GB space limitation and requires FILESTREAM to be enabled. If you install your own SQL Server Express instance, you must enable FILESTREAM.
- If you upgrade from an embedded database (14.3 MP1 and earlier) to 14.3 RU1 and later, you do not need to enable the FILESTREAM; the upgrade wizard or configuration wizard enables FILESTREAM for you automatically.
- The Microsoft SQL Server database does not require FILESTREAM to be enabled, but it is recommended to improve performance. For a local SQL Server database, the Management Server Upgrade and Installation Wizard can enable FILESTREAM for you. For a remote Microsoft SQL Server database, you enable FILESTREAM manually on the computer where the SQL Server database is installed.

If you run the upgrade wizard or the configuration wizard and the following message appears, click **Yes**, and enable FILESTREAM.

The FILESTREAM feature is not enabled for this remote Microsoft SQL Server database.

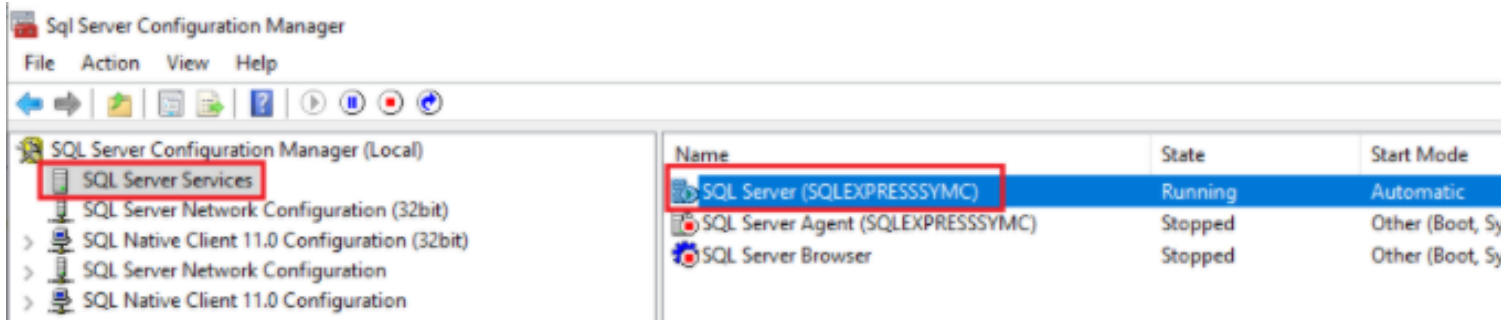
#### NOTE

Click **No** if you want to continue upgrading or installing and you do not want to enable the FILESTREAM feature at this time.

If you are upgrading, the Management Server Upgrade wizard closes. After you enable FILESTREAM, you must restart the upgrade wizard to continue the management server upgrade. On the Symantec Endpoint Protection Manager computer, click: `..\Symantec\Symantec Endpoint Protection Manager\bin\upgrade.bat`.

**To enable FILESTREAM manually:**

1. On the **Start** menu, expand **Microsoft SQL Server** and then click **SQL Server Configuration Manager**.
2. In the **SQL Server Configuration Manager** list of services, select **SQL Server Services**, and then locate the instance of SQL Server on which you want to enable FILESTREAM.



3. Right-click the instance, and then click **Properties**.
4. In the **SQL Server Properties** dialog box, click the **FILESTREAM** tab.
5. Select the **Enable FILESTREAM for Transact-SQL access** and click **Enable FILESTREAM for file I/O streaming access** check boxes.
6. Click **Apply > OK**.
7. Restart the SQL Server database service by selecting the instance of SQL Server and clicking **Restart**.

[FILESTREAM \(SQL Server\)](#)

## Reducing the database size to less than 10 GB before an upgrade to Microsoft SQL Server Express

The default Microsoft SQL Server Express database has a size limit of 10 GB for data files and log data. Data files include items such as installation packages, virus definitions, policies, alerts, and learned applications. When you upgrade from the embedded database (14.3 MP1 and earlier) with a size larger than 10 GB, the upgrade process to SQL Server Express cannot continue. If the Management Server Configuration Wizard detects that the database size is too large, you may see the following message:

The backup exceeds the allowed SQL Server Express 10 GB limit. You must first reconfigure the management server to import less data. Then run the restore again.

The estimated data in the embedded database exceeds the Microsoft SQL Server Express limit of 10 GB. To continue the upgrade, the wizard must first reduce the amount of data to less than 10 GB.

You must first decrease the space in the existing embedded database, using one of the following tasks:

- Click **Continue** so that the Management Server Configuration Wizard decreases the database size at the beginning of the upgrade process.
- Cancel the Management Server Configuration Wizard, reduce the database size yourself, and restart the wizard using the following steps.

**To reduce the amount of available database size manually:**

- **Step 1: Remove any replication partners that Symantec Endpoint Protection Manager does not use**

## Deleting sites

- **Step 2: Decrease the size of the logs and learned application data**  
Specifying the log size and how long to keep log entries in the database

Database Properties for karin-2012\SQLEXPRESS\SYMCD

General Log Settings Backup Settings

Specify the size of logs maintained in the database for the site.

**Management Server Log Settings**

System Administrative Log Limit:	10000	entries	Expires after:	60	days
System Client-Server Activity Log Limit:	10000	entries	Expires after:	60	days
Audit Log Limit:	10000	entries	Expires after:	60	days
System Server Activity Log Limit:	10000	entries	Expires after:	60	days

**Client Log Settings**

Client Activity Log Limit:	10000	entries	Expires after:	60	days
Security Log Limit:	10000	entries	Expires after:	60	days
Traffic Log Limit:	50000	entries	Expires after:	60	days
Packet Log Limit:	10000	entries	Expires after:	60	days
Control Log Limit:	20000	entries	Expires after:	60	days

**Risk Log Settings**

Delete risk events after:	60	days	Compress risk events after:	7	days
Delete acknowledged notifications after:	30	days	Delete unacknowledged notifications after:	30	days
Delete scan events after:	30	days	Delete commands after:	30	days

☒ Delete unused virus definitions ☒ Delete EICAR events

OK Cancel Help

Symantec Site Properties for Local Site (Site 71DP4Y2)

General LiveUpdate Passwords Data Collection Private Insight Server

**Site Settings**

Site Name: Site 71DP4Y2

Description:

Console Timeout: 1 hour

☐ Keep track of every application that the clients run

☐ Delete learned application data after: 30 days

The management console uses the first server in the list to send reports and notification. If the server is not available, the management console uses the next server in the list. You can change the priority of servers by using the Move Up and Move Down buttons.

71DP4Y2

Move Up

Move Down

OK Cancel Help

---

### [Enabling application learning](#)

- **Step 3: Change the default settings for the database maintenance schedule**

- a. Stop the management server.
- b. In the following file: `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\conf.properties`, decrease the number of seconds for the following entries.

```
scm.timer.objectsweep=1800
```

```
scm.timer.objectsweep.delay=60
```

Note: If these entries are not in the file, add them. This step increases the frequency that the database marks unwanted data as deleted.

[Symantec Endpoint Protection Manager: How is Database Maintenance scheduled?](#)

- c. Restart the management server and wait for several hours or longer.

[Stopping and starting the management server service](#)

- **Step 4: Schedule replication between all partners to occur at least once. Symantec recommends that you replicate more often**

[Installing a new site as a replication partner to an existing site](#)

- **Step 5: Wait for several hours after each scheduled replication before you restart the upgrade.**
- **Step 6: Rerun the database backup and then try to restore it.**

## **Making more disk space available to upgrade to the default Microsoft SQL Server Express database**

If the Symantec Endpoint Protection Manager computer does not have at least 10 GB of available disk space to upgrade to the Microsoft SQL Server Express database, you may see the following message:

The upgrade wizard cannot upgrade your embedded database to a Microsoft SQL Server Express database. Either the destination drive does not have enough available disk space, or the certificate is expired or will expire within 10 days. Make sure there is at least x of free disk space and that the certificate is current to continue.

You cannot continue the upgrade process, unless you make at least 10 GB of disk space available. To increase disk space, perform the following steps.

### **Step 1: Remove unused files and temporary files**

The Windows temporary files are located in:

- `C:\Windows\Temp`
- `C:\Users\<username>\AppData\Local\Temp`

### [Disk cleanup in Windows 10](#)

### **Step 2: Empty the Recycle Bin**

### **Step 3: Remove additional SEPM files**

1. If the previous steps do not reduce enough disk space, remove additional SEPM files.  
Stop the management server service using the Run command: `net stop semsrv`  
[Stopping and starting the management server service](#)
2. Move the following SEPM files to another disk drive:
  - `..\Symantec\Symantec Endpoint Protection Manager\Inetpub\ClientPackages`
  - `..\Symantec\Symantec Endpoint Protection Manager\Inetpub\content`
  - `..\Symantec\Symantec Endpoint Protection Manager\data\backup`
  - `..\Symantec\Symantec Endpoint Protection Manager\data\inbox`
3. Restart the management server service.

---

#### Step 4: Change database backup settings

- Make sure the **Number of database backups to keep** option is set to 1, the default.
- Keep **Back up logs** unchecked.

#### [Running automatic database backups](#)

#### Step 5: Move files that the Symantec Endpoint Protection Manager does not use to another disk drive.

If the certificate has expired, see: [Configuring encrypted communication between Symantec Endpoint Protection Manager and Microsoft SQL Server](#)

## Configuring encrypted communication between Symantec Endpoint Protection Manager and Microsoft SQL Server

Symantec Endpoint Protection Manager uses a certificate to authenticate communications between the Symantec Endpoint Protection (SEPM) and the Microsoft SQL Server Express or SQL Server databases. You must generate the certificate and import it into the Symantec Endpoint Protection Manager computer for SEPM to connect to either SQL Server database. If the certificate does not exist, is expired, or is about to expire, the connection between SEPM and the database fails.

You can install or upgrade the management server and either SQL Server database if you have not imported the certificate. However, the Management Server Configuration Wizard detects whether the certificate is already expired or expires within the next 30 days. SEPM sends a notification every day until the 30 days is over to remind the administrator to import the certificate. You may see the following message:

Within the next 30 days, Symantec Endpoint Protection Manager will no longer be able to connect to the Microsoft SQL Server database because SQL Server uses a certificate that is about to expire.

#### Step 1: Generate a self-signed certificate

If your organization does not already have a Certificate Authority (CA) signed certificate, you must generate one. This step describes how to generate and replace the default self-signed Symantec Endpoint Protection Manager (SEPM) certificate with a CA-signed certificate.

See [Use a signed certificate with Endpoint Protection Manager](#).

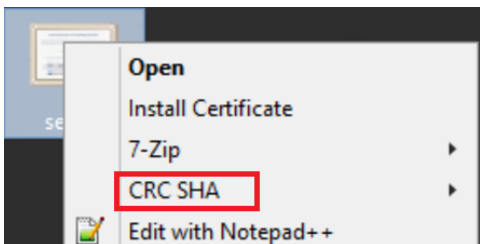
#### Step 2: Configure a permanent certificate for SQL Server

You must enable encrypted connections for an instance of the SQL Server Database Engine and must use SQL Server Configuration Manager to specify the certificate. See "Configure the SQL Server" at: [Enable encrypted connections to the Database Engine](#)

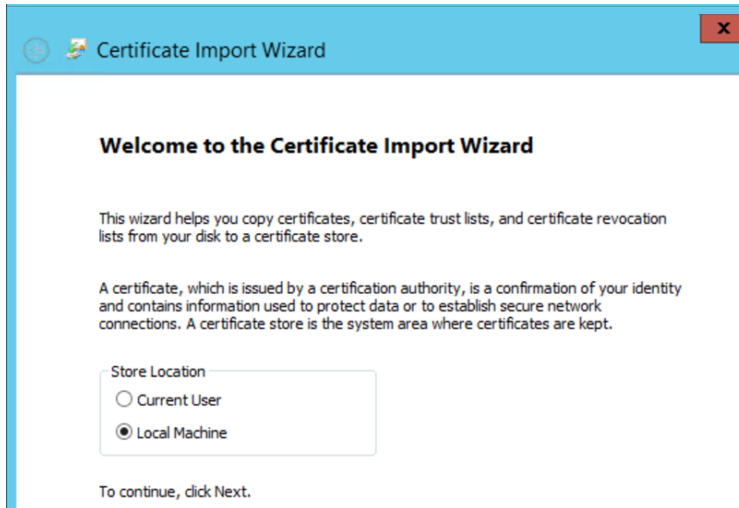
#### Step 3: Import the SQL Server certificate into Windows on the Symantec Endpoint Protection Manager computer

The management server computer must have the SQL Server public certificate provisioned. To provision the certificate on the management server computer, you import it into Windows. The server computer must be set up to trust the certificate's root authority.

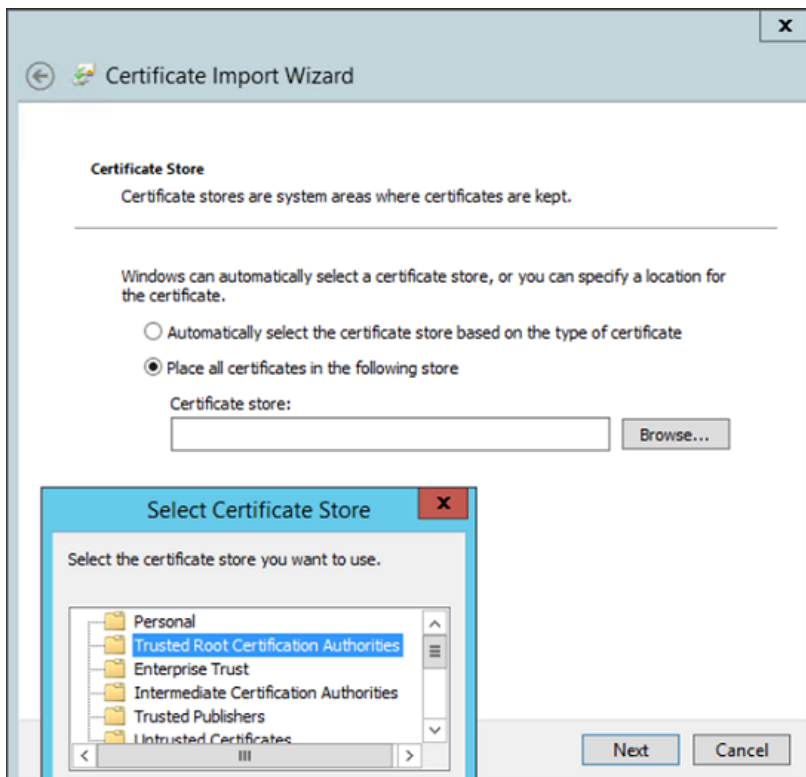
1. On the Windows Server where SEPM is installed, right click the certificate.

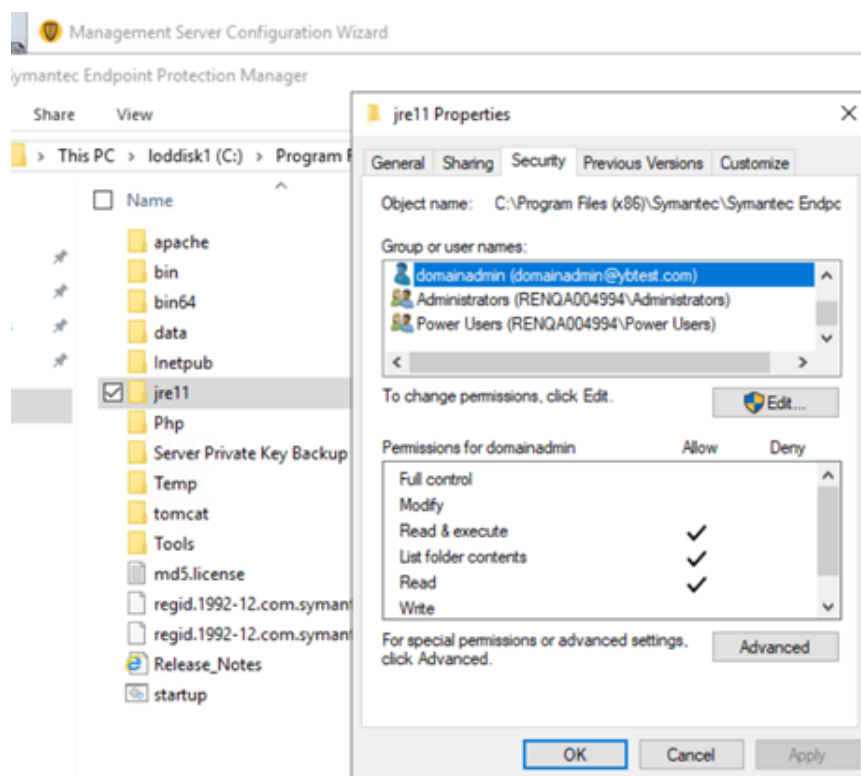


2. In the Certificate Import Wizard, follow the steps to import the certificate.  
Under **Store Location**, select **Local Machine**:



Select **Place all certificates in the following store**, click **Browse**, and in the Select Certificate Store dialog box, click **Trusted Root Certification Authorities**:





3. Click **OK**, and then click **Next**.

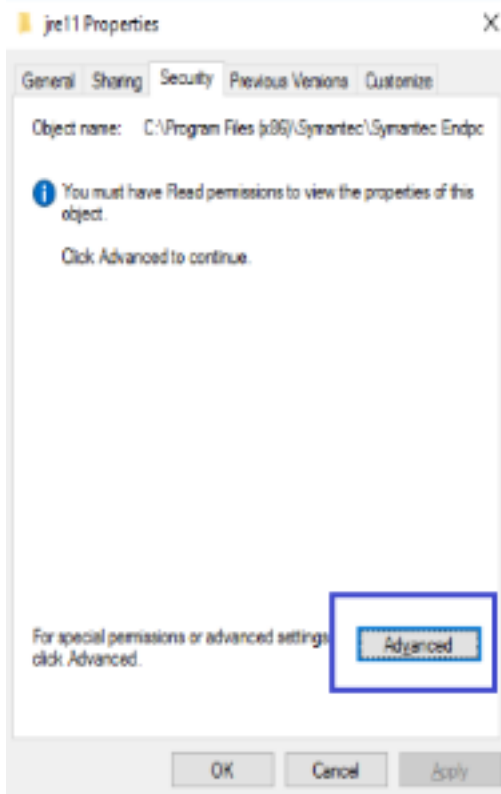
#### Step 4: Configure permissions for the jre11 folder

##### NOTE

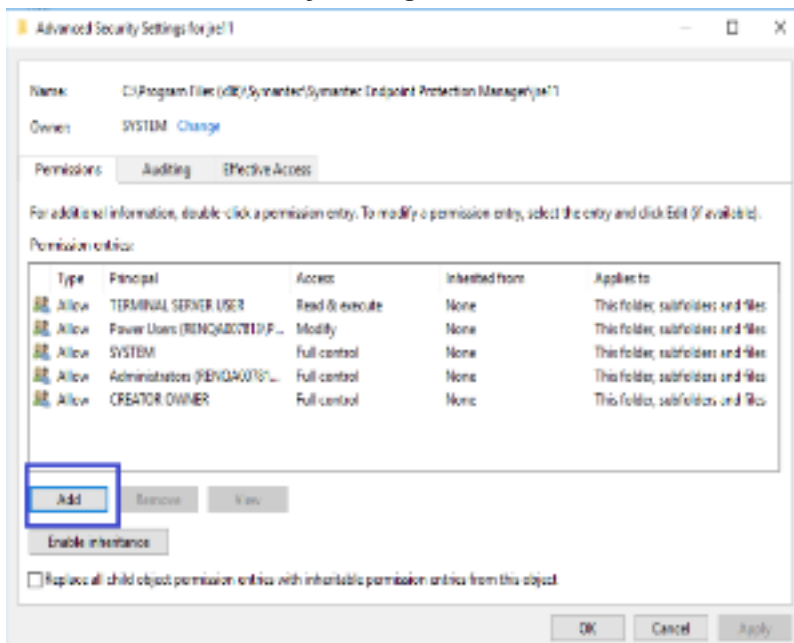
If your SQL Server is configured using a domain admin with Windows authentication, the domain admin needs to have **Read & execute**, **List folder contents**, and **Read** permissions for the jre11 folder on the Symantec Endpoint Protection Manager server.

1. On the Symantec Endpoint Protection Manager server, go to `...\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager` folder, right-click the jre11 folder, and click **Properties**.
2. In the file properties window, on the **Security** tab, click **Advanced**.

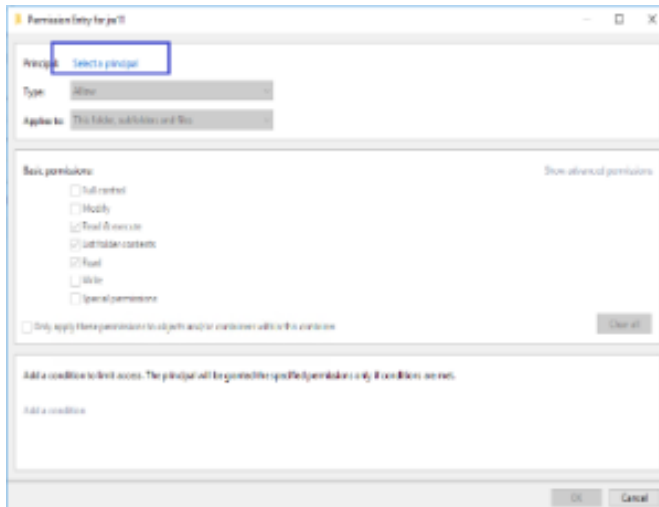




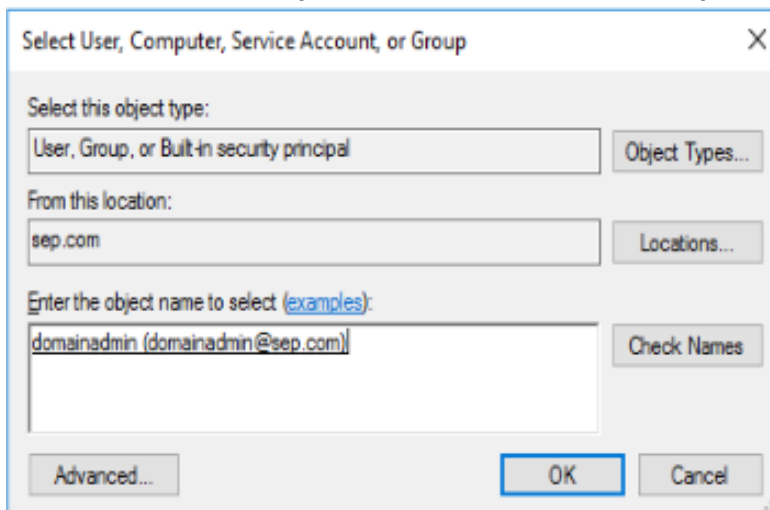
3. In the **Advanced Security Settings** window, on the **Permissions** tab, click **Add**.



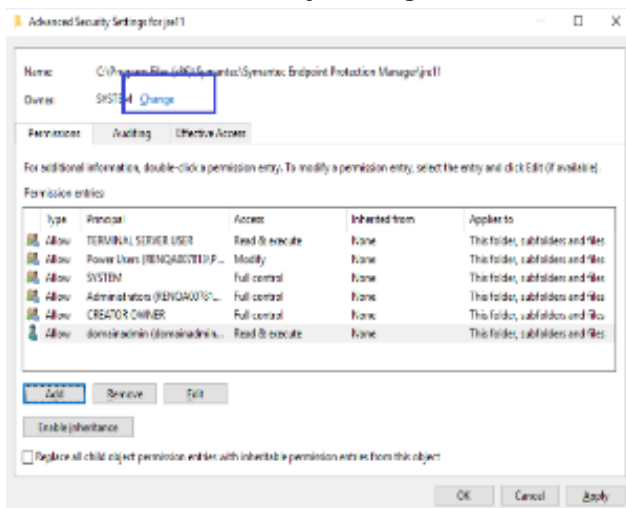
4. In the **Permissions Entry** window, click **Select a principal**.



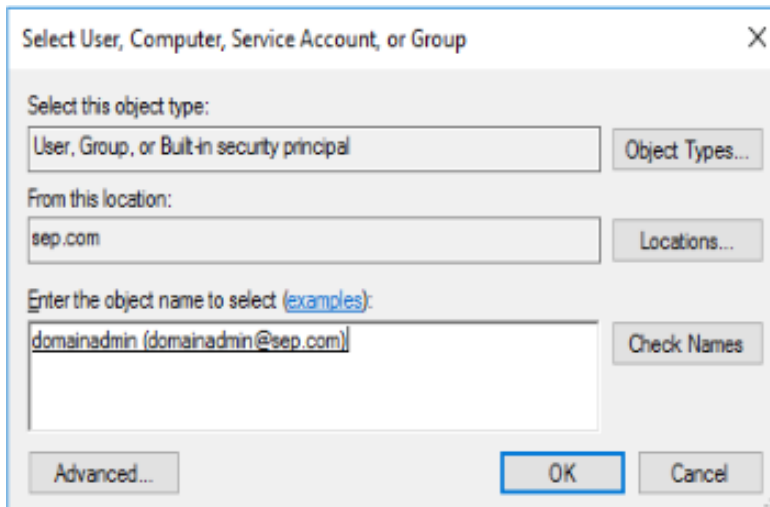
5. In the **Select User, Computer, Service Account, or Group** window, add the **domainadmin** user, and click **OK**.



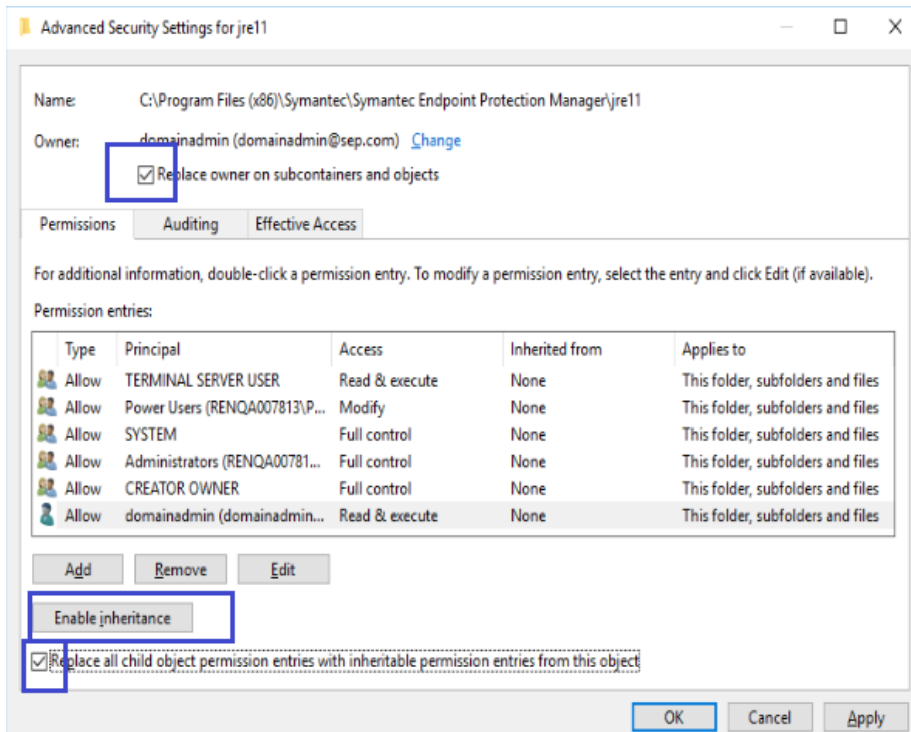
6. In the **Permissions Entry** window, click **OK**.
7. In the **Advanced Security Settings** window, on the **Permissions** tab, select **domainadmin**, and click **Change**.



8. In the **Select User, Computer, Service Account, or Group** window, add the **domainadmin** user again, and click **OK**.



9. In the **Advanced Security Settings** window, check **Replace owner on subcontainers and objects**, check **Replace all child object permission entries with inheritable permission entries from this object**, click **Enable inheritance**, and click **Apply**.



10. Click **Yes** and **OK** to confirm.
11. In the file properties window, make sure that the **domainadmin** user has now all required permissions, and click **OK**.

### Step 5: Open the Management Server Configuration Wizard and complete the Server Configuration with Windows Authentication option

To open the wizard, go to `...\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\bin` folder, and double-click `sca.exe` file.

Management Server Configuration Wizard

Step One: Database Server Authentication  
This step must be completed first.

Authentication type: Windows Authentication

Database server: renqa007813.sep.com

SQL server port: 1433

Windows user name: sepdomainadmin

Windows user password: \*\*\*\*\*

SQL Server client folder: C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\

Connect to database

Step Two: New Database Creation

Database name: sem5

Database data folder: C:\Program Files\Microsoft SQL Server\MSSQL14.MSSQLSERVER\MSSQL\DATA

< Back Next > Cancel

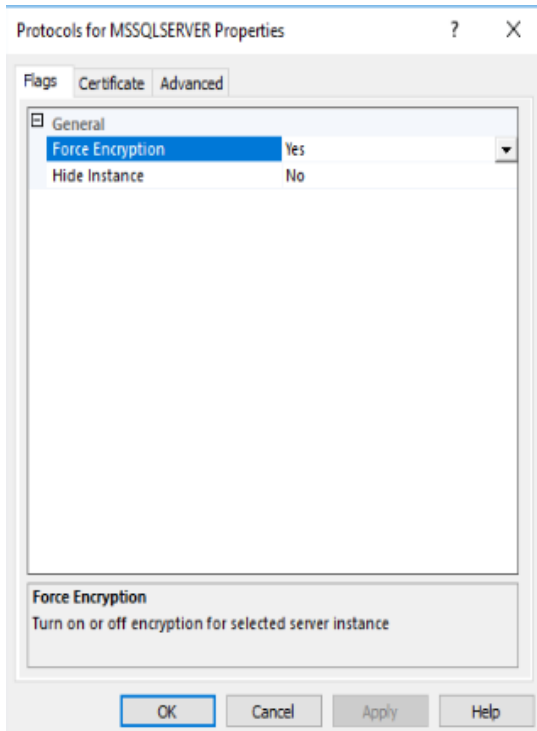
## Step 6: Check if the communication is encrypted and using the SQL Server certificate

1. On the management server, open the following file: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\tomcat\conf\Catalina\localhost\root.xml and make sure that **encrypt=true** and **trustServerCertificate=false**.

C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\tomcat\conf\Catalina\localhost\root.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<Context reloadable="false" privileged="true" crossContext="true" antiResourceLocking="false" antiJARLocking="false">
  <Resource validationQueryTimeout="60" validationQuery="SELECT count(*) FROM CONNECTION_TEST" username="domainadmin"
    url="jdbc:sqlserver://renqa007813.sep.com:1433;databaseName=sem5;integratedSecurity=true;encrypt=true;trustServerCertificate=false;domain=sep"
    type="javax.sql.DataSource" removeAbandonedOnBorrow="true" password="{V01}B7DAEBA1EF9473FAA7C9D103B5C3C712" name="jdbc/metadatabase"
    mssqlSocketReadTimeout="1800" maxWaitMillis="30000" maxTotal="150" maxIdle="50" logAbandoned="false" factory="com.sygate.scm.pool.ScmDataSourceFactory"
    driverClassName="com.microsoft.sqlserver.jdbc.SQLServerDriver" domain="sep" auth="Container"/>
</Context>
```

2. On the SQL Server, open **Protocols for MSSQLSERVER Properties**, and check if **Force Encryption=Yes**.



- On the SQL Server, run the following query, to check if the connection between Symantec Endpoint Protection Manager and SQL Server is encrypted:

```
SELECT session_id, connect_time, net_transport, encrypt_option, auth_scheme, client_net_address FROM sys.dm_exec_connections
```

Check if **encrypt\_option=TRUE**.

SQLQuery1.sql - RE...Administrator (53))

```
SELECT session_id, net_transport, encrypt_option, auth_scheme, client_net_address FROM sys.dm_exec_connections
```

100 %

Results Messages

	session_id	net_transport	encrypt_option	auth_scheme	client_net_address
1	51	Shared memory	TRUE	NTLM	<local machine>
2	52	TCP	TRUE	SQL	10.32.168.100
3	53	Shared memory	TRUE	NTLM	<local machine>
4	54	Shared memory	TRUE	NTLM	<local machine>
5	55	TCP	TRUE	SQL	10.32.168.100
6	58	TCP	TRUE	SQL	10.32.168.100
7	57	TCP	TRUE	SQL	10.32.168.100
8	59	TCP	TRUE	SQL	10.32.168.100
9	60	TCP	TRUE	SQL	10.32.168.100

---

## Upgrading an environment that uses multiple embedded databases and management servers

An environment that uses multiple embedded database and management servers has the following implications:

- The management servers do not use failover or load balancing for Symantec Endpoint Protection because the embedded database does not support failover or load balanced servers.
- The management servers are Symantec Endpoint Protection replication partners.

All sites have a computer on which you first installed the management server. You must upgrade this management server first, because it contains critical site information such as the encryption key or encryption password. You then upgrade the other management servers that you installed for replication.

### NOTE

As of 14.3 RU1, the Microsoft SQL Server Express database replaces the embedded database. SQL Server Express supports failover and load balancing.

To upgrade an environment that uses multiple embedded databases and management servers

1. Authenticate to and log on to the computer on which you installed the first Symantec Endpoint Protection Manager.  
Do not log on to Symantec Endpoint Protection Manager. If you use replication, you do not need to disable it first. Symantec Endpoint Protection does not allow replication if the product versions do not match.
2. Upgrade the management server.
3. Upgrade all additional management servers one by one.

## Stopping and starting the management server service

Before you upgrade, you must manually stop the Symantec Endpoint Protection Manager service on every management server in your site. After you upgrade, the service starts automatically.

### WARNING

If you do not stop the Symantec Endpoint Protection Manager service before you upgrade the server, you risk corrupting your existing Symantec Endpoint Protection database.

### NOTE

If you stop the management server service, the clients can no longer connect to it. If clients are required to communicate with the management server to connect to the network, they are denied access until this service is restarted.

For example, a client must communicate with the management server to pass a Host Integrity check.

### Upgrading to a new release

1. To stop the Symantec Endpoint Protection Manager service, click **Start > Settings > Control Panel > Administrative Tools > Services**.
2. In the **Services** window, under **Name**, scroll to and right-click **Symantec Endpoint Protection Manager**.
3. Click **Stop**.
4. Close the Services window.

### WARNING

Close the Services window or your upgrade can fail.

- 
5. Repeat this procedure for all installations of Symantec Endpoint Protection Manager.

**NOTE**

To start the Symantec Endpoint Protection Manager service, follow this procedure again, but click **Start** instead of **Stop**.

6. To stop the Symantec Endpoint Protection Manager service using the command line, from a command prompt, type:

```
net stop semsrv
```

7. To start the Symantec Endpoint Protection Manager service using the command line, from a command prompt, type:

```
net start semsrv
```

## Preventing replication during an upgrade

You should make sure that replication does not occur on any management servers that are configured as replication partners to the management server you are upgrading. If a replication partner launches replication during the upgrade, it may have unpredictable results.

To prevent replication during the upgrade, perform one of the following tasks:

- Reschedule replication to occur outside the upgrade period. Symantec recommends this method as it is simpler.
- Temporarily suspend replication before an upgrade, and restore it after the replication is over.

### Rescheduling replication

The advantage to modifying the schedule is that the other sites do not replicate, and they keep servicing the clients until the clients are upgraded. After the upgrade finishes, the sites can both test replication by forcing a one-time replication and change the schedule back to the previous set schedule and frequency.

Follow these best practices to modify the schedule:

- Document existing schedule and settings.
- Change the schedule to prevent replication from happening during upgrade window by scheduling it in the future or different day.
- Force replication so that schedule is picked up by all replication partners, or sites.

### [Changing the replication frequency and content](#)

### Suspending and restoring replication

You must log on to Symantec Endpoint Protection Manager and suspend replication at a minimum of two sites.

**WARNING**

Suspending replication is not the same as permanently deleting the replication partnership. If you delete the relationship and then reinstall the management server, the management servers perform a full replication instead of an incremental replication. [Deleting sites](#)

1. Stop the management server service.
2. In the console, click **Admin > Servers**.
3. Under **Local Site > Servers**, expand **Replication Partners** and select the management server.
4. Right-click the management server, and then click **Delete Replication Partner**.
5. Click **Yes**.
6. Repeat this procedure at all sites that replicate data.
7. Restore replication and restart the management server service.

### [Restoring replication](#)

### [Upgrade best practices for Endpoint Protection 14](#)

## Restoring replication

After you upgrade all management servers that had a replication relationship, you add the replication partner back. You must also re-add the management servers that were configured for failover and load balancing.

You only re-add replication partners on the computer on which you first upgraded the management server. The upgraded management server must also have previously been a replication partner in the same site farm.

After you add the replication partner back, Symantec Endpoint Protection Manager makes the databases consistent. However, some changes may collide.

### [How to resolve data conflicts between sites during replication](#)

If you have two separate, non-replicating sites, you can also use this option to convert one of the sites into a site which replicates with the other site.

1. On the console, click **Admin > Servers**.
2. Under **Servers**, expand **Local Site**, and under **Tasks**, click **Add Existing Replication Partner**.
3. In the welcome panel, click **Next**.
4. In the **Remote Site Information** panel, type the IP address or host name for the second management server, the system administrator's logon information, and then click **Next**.  
The system administrator's user name is `admin` by default.
5. Set the replication schedule and click **Next**.
6. Check which items to replicate, and then click **Next**.  
Client package replication uses large amounts of traffic and hard disk space.  
If you click **Yes**, the management server performs a full replication of data between the two replication partners.
7. When a message appears asking whether or not you have restored the database on the partner site, click one of the following options:
  - Click **No** to replicate only the data that changed since this partner relationship was disabled. Symantec recommends this option, especially if your network has low bandwidth.
  - Click **Yes** to perform a full replication of data between the two replication partners.
8. Click **Finish**.
9. Repeat this procedure for all computers that replicate data with this computer.  
Make sure that you restart the management server service after you restart replication.

### [Upgrade best practices for Endpoint Protection 14](#)

### [Upgrading to a new release](#)

## Choosing which method to upgrade the client software

You can upgrade the client using multiple ways. The method you should use depends on your environment and goals. For example, you might have a large number of clients or groups, or computers that run different versions of the client.

Some methods can take up to 30 minutes. Therefore, you may want to upgrade client software when most users are not logged on to their computers.



**Table 45: Methods to upgrade the client software**

Method	When to use	When not to use
AutoUpgrade (Recommended for smaller environments)	<ul style="list-style-type: none"> <li>When you have a smaller number of clients, such as 5,000 clients or fewer.</li> <li>When you need to schedule the upgrade to occur when the upgrade does not interrupt the users' work.</li> <li>When you use Symantec Endpoint Protection Manager and not a third-party application to deploy the client installation package.</li> <li>When you need to upgrade either Windows or Mac clients, but not Linux clients.</li> <li>When you want a simple upgrade method.</li> </ul> <a href="#">Upgrading client software with AutoUpgrade</a>	<ul style="list-style-type: none"> <li>When you have a larger number of clients. This method does not scale well.</li> <li>When you have a lot of groups, because it is time-consuming to click each group individually in the wizard.</li> <li>When you have a complicated upgrade schedule where you need a lot of granularity.</li> <li>When you need to upgrade Linux clients.</li> </ul> <a href="#">How to deploy the Symantec Endpoint Protection Linux client as part of a cloned drive image</a>
Export a client installation package (Recommended for larger environments)	<ul style="list-style-type: none"> <li>When you deploy the client installation package manually instead of with Symantec Endpoint Protection Manager.</li> <li>When you deploy the client installation package with an existing third-party deployment application instead of with Symantec Endpoint Protection Manager. To use this method, you should have this infrastructure already in place.</li> <li>When you need to upgrade Windows clients, Mac clients, and Linux clients.</li> </ul> <a href="#">Exporting client installation packages</a> <a href="#">Installing Windows client software using third-party tools</a>	<ul style="list-style-type: none"> <li>When you normally use Symantec Endpoint Protection Manager to update the clients.</li> </ul>
Client Deployment Wizard	<ul style="list-style-type: none"> <li>When you have a smaller number of clients, such as fewer than 250 clients.</li> <li>When you deploy the client using Symantec Endpoint Protection Manager and not a third-party application.</li> <li>When you want a simpler upgrade method.</li> </ul> <p>Use the <b>New Package Deployment</b>.</p> <a href="#">Installing Symantec Endpoint Protection clients with Remote Push</a>	<ul style="list-style-type: none"> <li>When you have a large network environment, as this method does not scale well.</li> </ul>
Download client installation files from the Broadcom <a href="#">Download Management</a> page.	<ul style="list-style-type: none"> <li>When you want to upgrade a few clients at a time in a few specific cases. For example: <ul style="list-style-type: none"> <li>If an issue occurs on a few computers with an older version of the client, and the newer version fixes the issue.</li> <li>If you have a smaller number of clients to upgrade and do not want to upgrade the management server.</li> </ul> </li> <li>When you need to upgrade Windows, Mac, and Linux clients.</li> <li>When you must deploy the client directly on the computer or by using a third-party deployment application instead of Symantec Endpoint Protection Manager.</li> </ul> <p>You download the standalone <b>All Clients</b> installation file from the Download Management page <a href="#">Symantec Getting Started</a> and scroll to <b>On-Premises Security Products</b>.</p> <a href="#">Installing an unmanaged Windows client</a>	<p>If you upgrade the client on computers with existing managed clients, the clients stay managed. However, if you deploy to new computers without an existing client, this method installs an unmanaged client only. You must convert the client to a managed client later to connect to the management server.</p> <a href="#">How do I replace the client-server communications file on the client computer?</a> <a href="#">Exporting the client-server communications file (Sylink.xml) manually</a>

[Upgrading to a new release](#)

---

# Upgrading client software with AutoUpgrade

## OVERVIEW

AutoUpgrade lets you automatically upgrade the Symantec Endpoint Protection client software on the Windows or Mac clients in a group.

With AutoUpgrade, Windows standard clients receive a delta upgrade package that Symantec Endpoint Protection Manager creates. This package is smaller than the full installation package. Windows that are embedded or VDI clients always receive the full installation package. These clients do not maintain a copy of the installer in the installer cache. Mac clients always receive the full installation package.

## AUTOUPGRADE BEST PRACTICES

Use the following best practices for using AutoUpgrade:

- Test the AutoUpgrade process before you attempt to upgrade a large number of clients in your production network. If you do not have a test network, you can create a test group within your production network. For this kind of test, you add a few non-critical clients to the test group and then upgrade them by using AutoUpgrade.
- To reduce bandwidth during peak hours, schedule AutoUpgrade for after hours in the **Upgrade Clients with Package** wizard, especially for client groups with reduced-size clients. For wide area networks, you should also set up the remote clients to receive the upgrade package from a remote web server.
- As of 14.3 RU2, LiveUpdate downloads client installation packages with critical fixes or security fixes that you can install without a change to the client version. For example, if you had installed 14.3 RU2 build 4870, and 14.3 RU2 build 5200 becomes available, you use the AutoUpgrade wizard to install build 5200. You do not need to upgrade the management server; just the clients. You still must restart the client after each upgrade.
- As of 14.3 RU2, both the Symantec Endpoint Protection clients and the Symantec Endpoint Protection Manager is localized in the following five languages only: English, French, Spanish, Portuguese, and Japanese. If you are using one of the five supported languages, no action is required; you can upgrade as usual. You can automatically upgrade the client language to English if the previous client's language is unavailable. If you choose a non-English language, the clients with an unsupported language do not get upgraded. This option is off by default. To enable this option, click **Clients** page > **Install Packages** page, click **Add a Client Install Package** > **Upgrade to English if unsupported language is unavailable**. This option applies to the Windows client only.

[Upgrading Symantec Endpoint Protection 14.3 RU2+ to a supported language](#)

- Since AutoUpgrade was first included in the Mac client with Symantec Endpoint Protection 14, you cannot upgrade with AutoUpgrade from a version earlier than 14.
- After you upgrade Symantec Endpoint Protection Manager, run LiveUpdate in the console at least once before you use AutoUpgrade to upgrade the clients.

[Checking that Symantec Endpoint Protection Manager has the latest content](#)

- AutoUpgrade can only install the Application Hardening feature (14.2 and later) on client computers when the following conditions are met:
  - You must enable **Maintain existing client features when updating** when you run **Upgrade Clients with Package**. This setting is enabled by default.
  - The client computer cannot have the Symantec Data Center Security agent installed.
  - The Virus and Spyware Protection feature is currently installed and selected for upgrade.
- If you want to change between the Windows client installation types: **Standard client**, **Embedded or VDI**, **Dark network**, at a later time after client installation, you **must** first uninstall the existing client software, reconfigure these settings, and then reinstall the new client package. You cannot change this setting using AutoUpgrade.

## CONFIGURING THE AUTOUPGRADE WIZARD

1. To upgrade client software with AutoUpgrade, in the console, click **Admin** > **Install Packages**.
2. Under **Tasks**, click **Upgrade Clients with Package**.

- 
3. In the **Upgrade Clients Wizard** panel, click **Next**, select the appropriate client installation package, and then click **Next**.
  4. Select the group or groups that contain the client computers that you want to upgrade, and then click **Next**.
  5. Select from where the client should download the package from the following options:
    - To download from the Symantec Endpoint Protection Manager server, click **Download from the management server**.
    - To download from a web server that is local to the computers that need to update, click **Download from the following URL (http or https)**. Enter the URL of the client installation package into the provided field.
  6. Click **Upgrade Settings** to specify upgrade options.
  7. On the **General** tab, under **Client Settings**, choose from the following options, depending on the client operating system:
    - For Windows:
      - In the **Select the version for this package** to choose a build (as of 14.3 RU2).
      - Use the drop-down menus to select options for **Maintain existing client features when updating** and **Install Settings**. If you deselect **Maintain existing client features when updating**, you can optionally add or remove features when upgrading.
    - For Mac, use the drop-down menu to select options for **Install Settings**.
    - For Windows, **Content Selection** lets you include content in the installation package. If you include content, the package is larger, but the client has up-to-date content immediately after installation. If you do not include content, the package is smaller, but the client must get content updates after installation.

You can also add an optional upgrade schedule. Without a schedule, the AutoUpgrade process begins after the wizard completes.
  8. On the **Notification** tab, customize the user notification settings.

You can customize the message that is displayed on the client computer during the upgrade. You can also allow the user to postpone the upgrade.
  9. Click **OK**, and then click **Next**.
  10. In the **Upgrade Clients Wizard Complete** panel, click **Finish**.
  11. To confirm the version number of the client software, after the upgrade completes, you can check the version to confirm a successful upgrade in one of the following ways:
    - In the console, click **Clients > Clients**, select the appropriate group, and change the view to **Client Status**.
    - On the Windows client, in the Symantec Endpoint Protection client interface, click **Help > About**.
    - On the Mac client, open the Symantec Endpoint Protection client interface. In the menu bar, click **Symantec Endpoint Protection > About Symantec Endpoint Protection**.

The client computer must restart after the upgrade. By default, the clients restart after installation. You can configure the restart options in the group's general settings to control how the clients in a group restart after AutoUpgrade. You can also restart the clients at any time by running a restart command from the management server.

[Restarting the client computers from Symantec Endpoint Protection Manager](#)

[Applying upgrade settings to other groups](#)

## CONFIGURING THE CLIENT UPDATE POLICY (Optional)

As of 14.3 RU3, you can upgrade a subset of the clients within a security group on different days for a measured rollout. You use the Client Upgrade policy and the following location conditions to target these subgroups: host name, user name, group name, whether a file exists, or operating system. For example, you can upgrade Windows 8 computers in the middle of the night when users are offline.

The Client Upgrade policy provides more granular schedule settings that overrides the upgrade schedule settings in the AutoUpgrade wizard. The policy retains all other AutoUpgrade wizard settings. You apply the Client Upgrade policy to the same group to which you apply the AutoUpgrade wizard.

[Upgrading client software with the Client Upgrade policy](#)

---

## Applying AutoUpgrade settings to other groups

You can copy existing AutoUpgrade client installation package upgrade settings from one group to another group. If you copy upgrade settings, you don't have to create the package settings for each group individually.

This option copies the following client install package settings:

- The client feature set
- Whether **Maintain existing client features when updating** is enabled or disabled
- The client installation settings
- The content selection
- The download source
- The upgrade schedule
- The settings and message text from the **Notifications** tab

The Windows settings apply to Windows clients and the Mac settings apply to Mac clients during AutoUpgrade. They also apply to any new client that joins the group.

If you apply the copied settings to a package that is already assigned to a target group, the copied settings override the target group's existing settings. If the target group has no assigned package, this option adds a client install package with the copied settings.

To apply upgrade settings to other groups

1. In the console, do one of the following tasks:

- Click **Clients > Install Packages**, select the group, and under **Tasks**, click **Apply current deployment settings to other groups**.
- Click **Clients**, right-click a group, and then click **Copy Deployment Settings**.

2. In the **Copy Deployment Settings** dialog box, click the new groups, click **OK**, and then click **Yes**.

[Upgrading client software with AutoUpgrade](#)

## Upgrading Symantec Endpoint Protection 14.3 RU2+ to a supported language

As of 14.3 RU2, both the Symantec Endpoint Protection Manager (SEPM) and the clients are translated into five languages only: English, Brazilian Portuguese, French, Japanese, and Spanish.

### UPGRADING THE SYMANTEC ENDPOINT PROTECTION MANAGER FROM A SUPPORTED TO AN UNSUPPORTED LANGUAGE

When you upgrade a SEPM with an unsupported Symantec Endpoint Protection Manager language, SEPM is automatically upgraded to English. However, you can upgrade SEPM to a supported language other than English, such as from Czech to French.

SEPM uses two components to display a language: the resource files and the system locale settings. To display SEPM in one of the supported languages other than English, SEPM must have both the resource file and the system format locale setting in the same language. If the resource file and the system locale setting do not match a supported language, SEPM is installed in English.

#### NOTE

Symantec recommends you follow this step before you upgrade the management server.

**To set the system format locale to the target migration language:**

1. Click the **Start -> Control Panel -> Clock and Region -> Region -> Formats** tab (Windows 10 and Windows Server 2019).

---

This step changes depending on which Windows version that SEPM runs on.

2. In the **Format** drop-down list, choose the target language, and then click **OK**.

You can choose any format for the target language. For example, if you want to upgrade to French, it makes no difference if you choose French (Algeria) or French (Belgium).

## UPGRADING THE CLIENTS FROM A SUPPORTED TO AN UNSUPPORTED LANGUAGE

To automatically upgrade clients with an unsupported language to English, check the **Upgrade 14.3+ clients to English if client language is not a supported** option in the AutoUpgrade wizard. If you do not check this option, clients with an unsupported language do not upgrade automatically. This option is available in an English Symantec Endpoint Protection Manager only.

**Mac:** Mac clients must be upgraded from an unsupported language to a supported language manually or using desktop management tools.

**Linux:** The Linux client continues to be translated into Japanese only.

### NOTE

If you automatically upgrade a client with an unsupported language to English, the client continues to display the date settings for definitions in English (14.3 RU1 and later). To work around this issue, uninstall the legacy client and manually install a new English client installation package. In addition, a fix is expected for clients that are upgraded automatically. [SEP-72481]

[Upgrading client software with AutoUpgrade](#)

## Installing Endpoint Protection client patches on Windows clients

### What are client patches and how do they work?

A client patch, or security fix, is a software patch for Symantec Endpoint Protection Windows clients that corrects a security vulnerability or functionality issue that exists in the client code. As new vulnerabilities and issues become known, Symantec delivers a client patch to fix the issue and uploads it to a LiveUpdate server (as of 14.3 RU2). Client patches are like any other type of content, like IPS signatures or virus and spyware definitions. You download client patches from the LiveUpdate server to the management server as an incremental delta (.dax) file. You then download the patches to clients in the same way as other content, using a LiveUpdate server, the management server, or a Group Update Provider (GUP).

[Choose a distribution method to update content on clients](#)

### NOTE

A client patch is not the same as a maintenance patch (MP) or a release update (RU). A client patch only addresses a possible security issue or client defect, and is delivered through LiveUpdate. A maintenance patch provides other updates or features, such as to offer support for new operating systems, and is delivered as a full installation download through the Broadcom [Download Management](#) page. In 14.3 RU2 and later, client patches have the same content as product updates. However, product updates are included in a full client installation package, whereas a client patch includes just the delta file.

[About Endpoint Protection release types and versions](#)

If the client and the management server versions match, the clients can get the client patches from a LiveUpdate server, a management server, or a GUP. If the client and the management server versions do not match, the clients get the client patches from a LiveUpdate server only, as in the case when a management server manages clients with multiple versions. If you want to use the management server or a GUP to download patches, you must update either the client or the management server version so that they are the same version.

The following table displays examples of whether or not the client can receive client patches from the management server, based on the version number of Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client.

**Table 46: Examples of which client versions download which client patches**

Management server version	Client version	Does the client download patches from the management server?
14.2	14.2	Yes
14.2	14.0.1 MP2	No
14.0.1 MP2	14.0.1 MP2	Yes
14.0.1 MP2	14.0.1 MP1	No
14.0.1 MP2	14.2	No

In 14.3 RU2 and later, LiveUpdate downloads not just client patches also feature updates. In this case, the client build does not have to match the management server. It can be older, the same, or newer.

#### [Upgrading client software with AutoUpgrade](#)

The language for the client must match the management server to download client patches. For example, a French management server that manages French, German, and simplified Chinese clients provides client patches to the French clients only. However, you can use AutoUpgrade to install a French, German, and Chinese client installation package, which has the client patches. And you can import and or use LiveUpdate to include these other languages' client installation packages and client patches.

#### **Installing client patches on Windows computers**

By default, LiveUpdate downloads client patches to Symantec Endpoint Protection Manager, which in turn installs the patches on the clients based on the distribution method you have configured for the other content types.

After a client downloads and installs a client patch, it continues to run the previous, unpatched version of the client until the client is restarted. Either the client end user must restart the computer, or you must run the restart command from the management server. The management server sends you a notification that indicates which clients require a restart.

To install client patches on Windows clients:

1. In the console, verify that LiveUpdate is configured to download the client patches to the management server.  
In the **Content Types to Download** dialog box, make sure that **Client patches** is checked.  
In 14.3 RU1 and earlier, this option was called **Client security patches**.  
[Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager](#)
2. To run a report to find out which release is installed on the client computers, run a **Protection Content Versions** report.  
[Generating a list of the Symantec Endpoint Protection versions installed in your network](#)
3. Verify that the LiveUpdate Settings policy is configured to download the patches to the clients.  
In a LiveUpdate Settings policy, under **Windows Settings**, click **Advanced Settings**. Make sure **Download client patches** is checked.  
**NOTE**  
Make sure that **Download delta content from a LiveUpdate server when available** is checked. This option merges the client patches from the current release with the content with the new patch, and then downloads only the difference, or the delta. Use this option when bandwidth to the clients is low.
4. Restart the client computers.  
[Restarting the client computers from Symantec Endpoint Protection Manager](#)

## **Upgrading the Symantec Linux Agent**

(For 14.3 RU1 and later)

---

As of version 14.3 RU1, the Linux client installer detects and uninstalls the legacy Linux client (earlier than 14.3 RU1) and then performs a fresh install. Old configurations will not be retained.

### To upgrade the Symantec Linux Agent

1. In Symantec Endpoint Protection Manager, create and download the installation package.  
[Exporting client installation packages](#)
2. Copy the downloaded package to the Linux device.
3. Navigate to folder location and run the following command to make the **LinuxInstaller** file executable:

```
chmod u+x LinuxInstaller
```

4. Run the following command to uninstall the existing agent and re-install the Symantec Linux Agent:

```
./LinuxInstaller
```

Run the command as root.

5. To verify the installation, navigate to `/usr/lib/symantec` and run `./status.sh` script to confirm that the modules are loaded and daemons are running:

```
./status.sh
Symantec Agent for Linux Version: 14.3.450.1000
Checking Symantec Agent for Linux (SEPM) status..
Daemon status:
cafagent          running
sisamdagent       running
sisidsagent       running
sisipsagent       running
Module status:
sisevt            loaded
sisap             loaded
```

## Updating the kernel modules for the Symantec Linux Agent

(For 14.3 RU1 and later)

Whenever a new Linux kernel update is released, the Symantec Linux Agent for that platform needs to be updated to support the new kernel. To make the process more efficient, the kernel modules of the Linux agent can now be updated by using the Linux repository.

### NOTE

Ensure that the agents can connect to the Symantec repository server (<https://linux-repo.us.securitycloud.symantec.com/>) to download the kernel module updates.

Whenever you run the `yum update` command on a RHEL, Amazon Linux, Oracle Linux, or CentOS system, the command also looks for new agent packages. If an update is available, the latest kernel module is downloaded and the agent is updated automatically. After the kernel module is updated, you must restart the instance for the update to take effect.

Alternatively, you can update the agent kernel module by running the following command in the instance. Open a terminal window with root privileges, navigate to `/usr/lib/symantec/` and run the following command:

```
/usr/lib/symantec/installagent.sh --update-kmod
```

For the Ubuntu systems, type the following commands:

1. To refresh and update local package database:

```
sudo apt-get clean
sudo apt-get update
```



- 
2. To upgrade to the latest kernel module:  
`/usr/lib/symantec/installagent.sh --update-kmod`  
Superuser privileges are required to perform this action.

In a restricted environment with no Internet connection, you can update the kernel modules in one of the following ways:

1. Manually transfer the latest KMOD package to a system that has no Internet connection, attach the KMOD package to the LinuxInstaller, and then run the LinuxInstaller.
  1. On a system that has Internet connection, download the KMOD package.  
`./LinuxInstaller -d`
  2. Manually copy and paste the KMOD package to the agent that you want to upgrade.
  3. List the attached packages.  
`./LinuxInstaller -l`
  4. Attach the new KMOD package to the LinuxInstaller.  
`tar czf - [KMOD-package-name] >> LinuxInstaller`
  5. Make sure that the new KMOD package is included in the list of attached packages.  
`./LinuxInstaller -l`
  6. Run the installer to update the kernel modules.  
`./LinuxInstaller -- --update-kmod`
2. Set up a local repository and edit the repository settings so that the agent uses the local repository instead of the default Symantec repository.
  1. Set up the local repository that hosts the KMOD packages.  
For information about how to create a local repository, refer to documentation of the respective Linux distribution that you are using.
  2. On the client computer, run the following command to redirect it to use the local repo:  
`./LinuxInstaller --local-repo <localrepo_url>`  
Example of the URL: `--local-repo 'http://<repo_ip_or_hostname:<port_optional>/sep_linux'`
  3. To update the KMOD, run:  
`./LinuxInstaller -- --update-kmod`

If you update the operating system kernel modules, you must also update the corresponding kernel module update for the Symantec Endpoint Protection client. Without the compatible kernel modules, the Symantec Endpoint Protection client may not work properly and some features may be disabled.

### [Upgrading the Symantec Linux Agent](#)

## Upgrading Group Update Providers

Use this procedure to upgrade the clients that are Group Update Providers.

To upgrade Group Update Provider clients

1. Upgrade the Symantec Endpoint Protection Manager server to the new version of the software.
2. Upgrade the clients that are Group Update Providers to the new version of the client software.
3. Update the rest of the clients to the new version of the client software.

### [Using Group Update Providers to distribute content to clients](#)

### [Upgrading to a new release](#)



---

## Upgrade resources for Symantec Endpoint Protection

**Table 47: Upgrade resources**

Item	Resource
Client installation package settings and features	You can configure client installation packages with a variety of settings and protection features. <a href="#">Symantec Endpoint Protection features based on platform</a> <a href="#">About the Windows client installation settings</a> <a href="#">Choosing which security features to install on the client</a>
Feature and policy descriptions	<a href="#">How Symantec Endpoint Protection technologies protect your computers</a> <a href="#">The types of security policies</a>
Feature dependencies	<a href="#">Symantec Endpoint Protection feature dependencies for Windows clients</a>
Manage product licenses	Symantec Endpoint Protection is licensed according to the number of clients that are needed to protect the computers at your site. <a href="#">Symantec Endpoint Protection product license requirements</a>
Additional resources	See the following articles: <ul style="list-style-type: none"><li>• <a href="#">Best practices for upgrading to the latest version of Symantec Endpoint Protection</a></li><li>• <a href="#">Download the latest version of Symantec software</a></li><li>• <a href="#">Release notes, new fixes, and system requirements for all versions of Endpoint Protection</a></li></ul>

[Upgrading to a new release](#)

---

## Licensing Symantec Endpoint Protection

---

Symantec Endpoint Protection (SEP) requires a paid license to receive security content updates, product updates and versions, and access to Technical Support. After you install Symantec Endpoint Protection Manager, you have 60 days to purchase enough license seats to cover all of your deployed clients.

[Maintenance entitlement overview for Symantec Endpoint Protection](#)

**Table 48: How to license Symantec Endpoint Protection**

Task	Description
Step 1: Purchase a license	<p>To purchase a new license, contact your <a href="#">preferred reseller</a>.</p> <p>See <a href="#">Symantec Getting Started</a>, and scroll down to <b>On-Premises Security Products</b>. If you haven't already done so, create a Broadcom Support Portal account.</p> <p>You must purchase a license in the following situations:</p> <ul style="list-style-type: none"><li>• You want to purchase Symantec Endpoint Protection.</li><li>• Your trial license expired.</li><li>• Your paid license expired.</li><li>• You deployed more clients than your license allows (over-deployed).</li></ul> <p>You license according to the number of clients that you need to protect the endpoints at your site.</p> <p><a href="#">How many Symantec Endpoint Protection licenses do I need?</a></p>
Step 2: Activate your purchased license	<p>After you purchase your license, you receive an email with a Symantec license file (.slf) or a license serial number, which is attached to the email as a .zip file. You must extract the .slf file from the .zip file. You need the serial number to activate the installation.</p> <ul style="list-style-type: none"><li>• You must log on to the Symantec Endpoint Protection Manager with a System Administrator account, such as the default account admin.</li><li>• Go to the <b>Admin &gt; Licenses</b> page to import and activate your SEP product license.</li></ul> <p><a href="#">Activating or importing your Symantec Endpoint Protection product license</a></p>

You can perform the following tasks to manage your licenses.

**Table 49: Licensing tasks**

Task	Description
Retrieve your serial number	If you have an existing license from Symantec and need to retrieve your serial number, see: <a href="#">Symantec to Broadcom Transition Guide - My Entitlements</a>
Renew your license	Contact your <a href="#">preferred reseller</a> See: <a href="#">Symantec Renewals FAQ</a>
Find out when your license expire and if you are overdeployed	<p>Check the status for each license that you imported into the console to see whether you need to renew a license or purchase more licenses.</p> <p>You can apply an existing license to a product upgrade.</p> <p><a href="#">Checking the license status in Symantec Endpoint Protection Manager</a></p>
Back up your license file	<p>Back up your license files to preserve them in case the database or the computer's hard disk becomes damaged.</p> <p><a href="#">Backing up and recovering your license files</a></p>
Recover your license file	<p>You can recover the license file if you accidentally delete it.</p> <p><a href="#">Backing up and recovering your license files</a></p>

Task	Description
Send notifications when licenses are expiring	By default, Symantec Endpoint Protection sends the administrator a preconfigured notification to administrators about expired licenses and other license issues. <a href="#">What are the types of notifications and when are they sent?</a>
Check the product license requirements	Learn what are the license requirements for the computers that you want to protect. A license lets you install the Symantec Endpoint Protection client on a specified number of computers. <a href="#">What does a product license cover?</a> <a href="#">Symantec Endpoint Protection product license terminology</a> <a href="#">About multi-year licenses</a>

## Checking the license status in Symantec Endpoint Protection Manager

You can find out whether the management server uses a trial license or a paid license. You can also obtain the following license information for each paid license that you imported into the console:

- License serial number, total seat count, expiration date
- Number of valid seats
- Number of deployed seats
- Number of expired seats
- Number of over-deployed clients

The trial license status only provides limited information that is related to the expiration date.

1. To check whether you have a paid license or trial license, in the console, do one of the following tasks:
  - Click **Admin > Licenses**.
  - Click **Home > Licensing Details**.
2. To check the license expiration date, in the console, click **Admin > Licenses**.

[Licensing Symantec Endpoint Protection](#)

[Activating or importing your Symantec Endpoint Protection product license](#)

## Backing up and recovering your license file (.slf)

You should back up your license file in case the database or the console computer's hard disk becomes damaged.

After you receive the license file, save it to a computer that can be accessed from the Symantec Endpoint Protection Manager console. Many users save the license on the computer that hosts Symantec Endpoint Protection Manager. Many users also save a copy of the license to a different computer or removable storage media for safekeeping.

### To back up your license file

1. Copy the **.slf** license files from the directory where you saved the files to another computer of your choice.

### To recover your license file

- Do one of the following tasks:
  - a. On the Symantec Endpoint Protection Manager console **Admin** page, click **Licenses** and then under **Tasks**, click **Recover a deleted license**. On the **License recovery** panel, check the box next to the deleted license you want to recover, and then click **Submit**.
  - b. Retrieve the license file from the following default location: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Inetpub\license. When you import the license file using the Licensing Activation Wizard, Symantec Endpoint Protection Manager places a copy of the file in this folder.
  - c. Go to the [Symantec Endpoint Security](#) website and click **My Entitlements**. For more information, see [Symantec to Broadcom Transition Guide - My Entitlements](#)

## Purging obsolete clients from the database to make more licenses available

Symantec Endpoint Protection Manager can incorrectly display an over-deployed license status due to obsolete clients. These are database entries for the clients that no longer communicate with Symantec Endpoint Protection Manager in the protected environment. Clients can be rendered obsolete for many reasons, such as when you upgrade the operating system, decommission a computer, or change the hardware configuration.

If your license reports show more seats are licensed than known to be deployed, you should purge the database of obsolete clients. Obsolete clients count against the product license, so it is important to purge obsolete clients as soon as they are created. By default, purging occurs every 30 days. You can shorten the interval between purge cycles to more quickly purge the obsolete clients. You reset the interval as needed to suit your long-term needs after the purge cycle completes.

In non-persistent Virtual Desktop Infrastructures (VDIs), you can set a separate time period for purging the non-persistent clients. This setting purges the offline clients that have not connected during the time period that you set. Non-persistent offline clients do not affect the license count.

1. In the console, on the **Admin** page, click **Domains**, right-click the domain, and click **Edit Domain Properties**.
2. On the **General** tab, change the **Delete clients that have not connected for specified time** setting from the default of **30** to **1**.  
  
You do not need to set the option to purge the non-persistent clients for licensing purposes. The non-persistent clients that are offline do not count toward the license total.
3. Click **OK**.
4. Wait 24 hours and then revert the settings to 30 days or to another interval that suits your requirements.

[Purging obsolete non-persistent VDI clients to free up licenses](#)

Licensing Symantec Endpoint Protection

## What does a Symantec Endpoint Protection license cover?

The number of Symantec Endpoint Protection licenses are enforced according to the following rules:

**Table 50: Licensing enforcement rules**

Where applies	Rule
Term of license	The term of the license starts from the time and date of activation until midnight of the last day of the licensing term. If you have multiple sites, the license expires on the day and the time of the westernmost Symantec Endpoint Protection Manager database.
Symantec Endpoint Protection components	A Symantec Endpoint Protection license applies to the Symantec Endpoint Protection clients. For instance, in a network with 50 computers, the license must provide for a minimum of 50 seats. Instances of Symantec Endpoint Protection Manager do not require a license. Symantec Endpoint Protection Manager does not require that the client has a license to access the management server. An unlicensed client that connects to the management server is given a license. You must ensure that you have purchased enough license seats to cover each client computer.

Where applies	Rule
Sites and domains	A Symantec Endpoint Protection product license is applied to an entire installation regardless of the number of replicated sites or domains that compose the installation. For instance, a license for 100 seats covers a two-site installation where each site has 50 seats. If you have not implemented replication, you may deploy the same .slf file to multiple Symantec Endpoint Protection management servers. The number of clients reporting to your management servers must not exceed the total number of licensed seats.
Platforms	License seats apply to clients running on any platform, whether the platform is Windows, Mac, or Linux.
Products and versions	License seats apply equally across product versions.

For information on licensing the clients that access the third-party server software, such as Microsoft SQL Server, contact the software vendor.

[Licensing Symantec Endpoint Protection](#)

[Purging obsolete non-persistent VDI clients to free up licenses](#)

## About multi-year licenses

When you purchase a multi-year license, you receive a set of license files equal to the number of years your license is valid. For instance, a three-year license consists of three separate license files. When you activate a multi-year license, you import all of the license files during the same activation session. Symantec Endpoint Protection Manager merges the separate license files into a single activated license that is valid for the purchased duration.

While not recommended, it is possible for you to activate fewer than the full complement of license files. In this case, Symantec Endpoint Protection Manager merges the files and applies the duration of the license file that expires last. For instance, a three-year license that is activated with only the first two files indicates a duration of only two years. When you activate the third file at a later date, Symantec Endpoint Protection Manager accurately reports the full duration of the license as three years. In all cases, the number of seats remains consistent with the number of seats that you purchased.

When Symantec Endpoint Protection Manager merges files, it deletes the shortest duration files and keeps the longest duration file for internal license-keeping functions. If you think that Symantec Endpoint Protection Manager inappropriately deleted a license, recover and reactivate the deleted license.

You can see the license serial numbers of shorter duration that are associated with the active license. On the **Admin** page, click **Licenses** and then click the activated license. The associated licenses appear in the **Associated Licenses** column.

[Licensing Symantec Endpoint Protection](#)

## Symantec Endpoint Protection product license terminology

You must purchase a license that covers each deployed client. One license covers all clients regardless of platform and version.

The following terminology applies to Symantec product licenses:

Serial number	A license contains a serial number that uniquely identifies your license and associates the license with your company. The serial number can be used to activate your Symantec Endpoint Protection license.
Deployed	Deployed refers to the endpoint computers that are under the protection of the Symantec Endpoint Protection client software. For example, "We have 50 deployed seats" means that 50 endpoints have client software installed on them.
Activate	You activate your Symantec Endpoint Protection product license to enable unrestricted access to all program functionality. You use the License Activation wizard to complete the activation process. <a href="#">Activating or importing your Symantec Endpoint Protection product license</a>

Seat	A seat is a single endpoint computer that the Symantec Endpoint Protection client software protects. A license is purchased and is valid for a specific number of seats. "Valid seats" refers to the total number of seats that are specified in all of your active licenses.
Trial license	A trial license refers to a fully functioning installation of Symantec Endpoint Protection operating within the free evaluation period. If you want to continue using Symantec Endpoint Protection beyond the evaluation period, you must purchase and activate a license for your installation. You do not need to uninstall the software to convert from trialware to a licensed installation. You must get trial license from your sales account representative. The evaluation period is 60 days from the initial installation of Symantec Endpoint Protection Manager.
Over-deployed	A license is over-deployed when the number of deployed clients exceeds the number of licensed seats.

Understanding license requirements is part of planning your Symantec Endpoint Protection installation and managing your product licenses after installation.

### [Licensing Symantec Endpoint Protection](#)

## Licensing an unmanaged Windows client

Unmanaged clients do not require the manual installation of a license file, and they do not count towards the total seat count for a paid license. However, to enable the submission of reputation data from an unmanaged Windows client, you must install a paid license on the unmanaged client. Unmanaged Mac clients and Linux clients do not submit reputation data.

1. Locate and create a copy of your current Symantec Licensing File (.slf).

Use the same file that you used to activate your license on Symantec Endpoint Protection Manager.

2. In the client computer, place the copied license file into the Symantec Endpoint Protection client inbox (default location):

C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox\

By default, the folder in which the inbox appears is hidden, so use Folder Options to enable the showing of hidden files and folders.

If the license file is invalid or the license installation failed, the license appears in a new folder called `Invalid`. If the file is valid, it is automatically removed from the inbox after it is processed.

3. To verify that you applied the license correctly, check that no files appear in the inbox folder.
4. Check that the .slf file is in the following folder (default location):

C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Config

You can also include the .slf file as part of a third-party deployment package.

---

## Managing the client-server connection

---

After you install the client, the management server automatically connects to the client computer.

**Table 51: Tasks to manage connections between the management server and the clients**

Action	Description
Check whether the client is connected to the management server	You can check the client status icon in the client and in the management console. The status icon shows whether the client and the server communicate. <a href="#">Checking whether the client is connected to the management server and is protected</a> A computer may have the client software installed, but does not have the correct communications file. <a href="#">How does the client computer and the management server communicate?</a> <a href="#">How do I replace the client-server communications file on the client computer?</a>
Check that the client gets policy updates	Check that the client computers get the most current policy updates by checking the policy serial number in the client and in the management console. The policy serial number should match if the client can communicate with the server and receives regular policy updates. You can perform a manual policy update and then check the policy serial numbers against each other. <a href="#">Using the policy serial number to check client-server communication</a> <a href="#">Updating client policies</a>
Change which method you use to download policies and content to the clients	You can configure the management server to push down policies to the client or for the clients to pull the policies from the management server. <a href="#">Updating policies and content on the client using push mode or pull mode</a>
Decide whether to use the default management server list	You can work with an alternative list of management servers for failover and load balancing. The management server list provides a list of multiple management servers that clients can connect to. <a href="#">Configuring a management server list for load balancing</a>
Configure communication settings for a location	You can configure separate communication settings for locations and for groups. <a href="#">Configuring communication settings for a location</a>
Troubleshoot management server connectivity problems	If the management server and the client do not connect, you can troubleshoot connection problems. <a href="#">Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client</a>

For more information, see the following article: [About the communication ports that Symantec Endpoint Protection uses](#)

## Configuring management servers and the server-client connection

Use this section to:

- Configure the connection between the management server and the client.
- Improve client and server performance.
- Update server certificates and maintaining the client-server connection
- Integrate the Symantec Endpoint Protection Manager with third-party servers.

### Setting up HTTPS communications between a Symantec Endpoint Protection Manager and the clients

Symantec Endpoint Protection Manager uses an Apache web server to communicate with clients and provide reporting services. For new installations of Symantec Endpoint Protection 14, HTTPS communications are enabled by default.

HTTPS is a secure protocol that uses a certificate to sign and encrypt data, which provides for the confidentiality and the integrity of the communications.

**Table 52: Configuring HTTPS communication to the client**

Step	Description
Step 1: Check that the default HTTPS port is available	By default, HTTPS traffic uses port 443. In some networks, port 443 may already be bound to another application or service. Before you enable HTTPS communication, you must check to see if the default port is available. <a href="#">Verifying port availability</a>
Step 2: Change the default HTTPS port as needed	If port 443 is not available, choose an unused port from the high port range (49152-65535). Configure the management server to use the new port. Update the management server list to reflect the new port. <a href="#">Changing the HTTPS port for Apache for client communication</a> <a href="#">Configuring a management server list for load balancing</a>
Step 3: Enable HTTPS communication to the client	Edit the Apache httpd.conf file to allow HTTPS communication to the client. Test the connection, and then switch the clients to HTTPS communication. <a href="#">Enabling HTTPS client-server communications</a>

#### [Managing the client-server connection](#)

### Verifying port availability

Some Symantec Endpoint Protection Manager configurations require that you change a default port assignment to prevent a conflict with other applications or services. Before you assign a new port, you must check to be sure that another application or service does not use the new port.

Open a command prompt and enter the following case-sensitive command:

```
netstat -an | find ":port" | find "LISTENING"
```

Where port represents the port number for which you want to check availability. For example, to see if port 443 is available, enter:

```
netstat -an | find ":443" | find "LISTENING"
```

If the `netstat` command returns a result, you must find an unused port. You use the same command, but replace port with the port of your choice. If this command yields no results, then the port is free to use.

#### [Changing the HTTPS port for Apache for client communication](#)

#### [Setting up HTTPS communications between a Symantec Endpoint Protection Manager and the clients](#)

#### [Protecting client-to-server communication](#)

### Changing the HTTPS port for Apache for client communication

The default HTTPS port for Apache is port 443. If Symantec Endpoint Protection Manager hosts other HTTPS websites, port 443 may already be assigned to one of these websites. You should use a different port for new installations to minimize conflict with any applications that already use the default port 443. If you want clients to use the default port to communicate with Symantec Endpoint Protection Manager, you should first verify that port is available.



---

## NOTE

If you customize the HTTPS port number after you deploy the client software, the clients lose communication with the management server. They reestablish communication after the next client update from the server, which contains the new connection information. You can also use a Communication Update Package.

### [Restoring client-server communications with Communication Update Package Deployment](#)

After you complete this procedure, you enable HTTPS client-server communications.

To change the HTTPS port for Apache for client communication

1. In a text editor, open the following file:

SEPM\_Install\apache\conf\ssl\sslForClients.conf

SEPM\_Install by default is C:\Program Files\Symantec\Symantec Endpoint Protection Manager.

## NOTE

The enclosing folder SEPM\_Install\apache\conf\ssl\ may be read-only. In that case, you may need to uncheck **Read-only** in the folder properties.

2. Edit the following lines and replace the default of 443 with the new port number:

```
Listen 443
```

```
<VirtualHost_default_: 443>
```

3. Save the file and close the text editor.

### [Verifying port availability](#)

### [Enabling HTTPS client-server communications](#)

### [Setting up HTTPS communications between a Symantec Endpoint Protection Manager and the clients](#)

### [Protecting client-to-server communication](#)

## Enabling HTTPS client-server communications

You edit the httpd.conf file to enable secure communication between the Symantec Endpoint Protection Manager server and the clients using the HTTPS protocol.

If you need to use an alternate port for secure communication, you must change the port assignment in Symantec Endpoint Protection Manager first.

For new installations of Symantec Endpoint Protection 14.x, HTTPS client-server communications is enabled by default.

1. To enable HTTPS for the Apache web server, in a text editor, open the following file:

SEPM\_Install\apache\conf\httpd.conf

SEPM\_Install by default is C:\Program Files\Symantec\Symantec Endpoint Protection Manager.

2. Find the following text string and remove the hash mark (#):

```
#Include conf/ssl/sslForClients.conf
```

3. Save and then close the file.
4. Restart the **Symantec Endpoint Protection Manager Webserver** service.

Stopping and restarting the Symantec Endpoint Protection Manager Webserver service also stops and restarts the Symantec Endpoint Protection Manager service.

### [Stopping and starting the Apache Web server](#)

- 
5. To verify HTTPS works correctly, enter the following URL in a web browser:

`https://SEPMServer:port/secars/secars.dll?hello,secars`

Where SEPMServer is the server host name for Symantec Endpoint Protection Manager and port is the HTTPS port number. By default, HTTPS traffic uses port 443.

6. If the browser displays the word **OK**, the HTTPS connection is successful.

If a page error displays, repeat the previous steps and check that you formatted all strings correctly. Also check that you entered the URL correctly.

If you did not update the management server with a certificate authority-signed certificate and private key pair, the web browser displays a warning that the certificate is not trusted. The same warning appears when you access the website from a URL that is different than the subject name on the management server certificate, which is expected.

7. To switch the clients to use HTTPS for communication with Symantec Endpoint Protection Manager, in the Symantec Endpoint Protection Manager console, on the **Policies** tab, click **Policy Components > Management Server Lists**.
8. Double-click the management server list that your client groups and locations use. If you only have the default management server list, duplicate it, and then double-click the new list to edit it.

You can also click **Add a Management Server List**, under **Tasks**. Add the server information under **Management Servers**, **Add > New Server**. You can add one **New Server** entry for server IP address, and one for server name.

[Copying and pasting a policy on the Policies page](#)

9. Click **Use HTTPS protocol**.

Only click **Verify certificate when using HTTPS protocol** if you have previously updated the management server with a Certificate Authority-signed certificate and a private key pair.

[Best practices for updating server certificates and maintaining the client-server connection](#)

#### NOTE

If you used a custom HTTPS port number in the `sslForClients.conf` file, edit the server from the list of management servers. Click **Customize HTTPS port**, and then edit the port to match the number you previously used.

Click **OK** to save the custom port.

10. Click **OK** to save your management server list.
11. If you edited a copy of the default management server list, right-click it, click **Assign**, and then assign it to every group and location.

[Assigning a management server list to a group and location](#)

12. On the Symantec Endpoint Protection client, click **Help > Troubleshooting > Server Connection Status**.
13. Under **Last Attempted Connection** and **Last Successful Connection**, confirm the display of both the server address and the port number for HTTPS communications.
14. Click **Connect Now** to force an immediate connection, if desired.

[Changing the HTTPS port for Apache for client communication](#)

[Setting up HTTPS communications between a Symantec Endpoint Protection Manager and the clients](#)

[Protecting client-to-server communication](#)

## Improving client and server performance

Symantec Endpoint Protection Manager includes various features that enable you to increase the client performance and server performance while still maintaining a high level of security.

**Table 53: Tasks to improve performance on the server and on the client**

Task	Description
Change client-server communication settings	<p>Use pull mode instead of push mode to control how often the management server downloads policies and content updates to the client computers. In pull mode, the management server can support more clients. Increase the heartbeat interval so that the client and the server communicate less frequently. For fewer than 100 clients per server, increase the heartbeat to 15-30 minutes. For 100 to 1,000 clients, increase the heartbeat to 30-60 minutes. Larger networks might need a longer heartbeat interval. Increase the download randomization to between one and three times the heartbeat interval.</p> <p><a href="#">Updating policies and content on the client using push mode or pull mode</a></p> <p>For more information about setting heartbeat intervals, see the <a href="#">Symantec Endpoint Sizing and Scalability Best Practices</a> white paper.</p>
Randomize and reduce the number of content updates	<p>Content updates vary in size and frequency, depending on the content type and availability. You can reduce the effect of downloading and importing a full set of content updates by using the following methods:</p> <ul style="list-style-type: none"><li>• Distribute the client load across multiple management servers. <a href="#">Configuring a management server list for load balancing</a></li><li>• Use alternative methods to distribute the content, such as a Group Update Provider or third-party distribution tools. A Group Update Provider helps you conserve bandwidth by offloading processing power from the server to a client that downloads the content. <a href="#">Using Group Update Providers to distribute content to clients</a> <a href="#">Using third-party distribution tools to update client computers</a></li><li>• Randomize the time when LiveUpdate downloads content to the client computers. <a href="#">Randomizing content downloads from a LiveUpdate server</a> <a href="#">Randomizing content downloads from the default management server or a Group Update Provider</a></li><li>• Download content updates when users are not actively using the client computer. <a href="#">Configuring Windows client updates to run when client computers are idle</a></li></ul>
Adjust scans to improve computer performance	<p>You can change some scan settings to improve the computers' performance without reducing protection. For example, you can configure scans to ignore trusted files or to run when the computer is idle.</p> <p><a href="#">Adjusting scans to improve computer performance</a></p> <p><a href="#">Customizing Auto-Protect for Windows clients</a></p> <p><a href="#">Advanced Scanning and Monitoring</a></p>

Task	Description
Reduce database client log volume	<p>You can configure the logging options to optimize storage requirements and comply with company policies that control retention of logged data.</p> <p>The database receives and stores a constant flow of entries into its log files. You must manage the data that is stored in the database so that the stored data does not consume all the available disk space. Too much data can cause the computer on which the database runs to crash.</p> <p><b>You can reduce the volume of log data by performing the following tasks:</b></p> <ul style="list-style-type: none"> <li>• Upload only some of the client logs to the server, and change the frequency with which the client logs are uploaded. <a href="#">Specifying client log size and which logs to upload to the management server</a></li> <li>• Specify how many log entries the client computer can keep in the database, and how long to keep them. <a href="#">Specifying the log size and how long to keep log entries in the database</a></li> <li>• Filter the less important risk events and system events out so that less data is forwarded to the server. <a href="#">Modifying log handling and notification settings on Windows computers</a></li> <li>• Reduce the number of clients that each management server manages. <a href="#">Configuring a management server list for load balancing</a> <a href="#">Installing Symantec Endpoint Protection Manager</a></li> <li>• Reduce the heartbeat frequency, which controls how often the client logs are uploaded to the server <a href="#">Updating policies and content on the client using push mode or pull mode</a></li> <li>• Increase the amount of hard disk space in the directory where the log data is stored before being written to the database. <a href="#">About increasing the disk space on the server for client log data</a></li> </ul>
Perform database maintenance tasks	<p>To increase the speed of communication between the client and the server, you should schedule regular database maintenance tasks.</p> <p><a href="#">Scheduling automatic database maintenance tasks</a></p>

## About server certificates

Certificates are the industry standard for authenticating and encrypting sensitive data. To prevent the reading of information as it passes through routers in the network, data should be encrypted.

To communicate with the clients, the management server uses a server certificate. For the management server to identify and authenticate itself with a server certificate, Symantec Endpoint Protection Manager encrypts the data by default. However, there are situations where you must disable encryption between the server and the client.

[Best practices for updating server certificates and maintaining the client-server connection](#)

[Update the server certificate on the management server without breaking communications with the client](#)

You may also want to back up the certificate as a safety precaution. If the management server is damaged or you forget the keystore password, you can easily retrieve the password.

[Backing up a server certificate](#)

[Updating or restoring a server certificate](#)

[Generating a new server certificate](#)

**The management server supports the following types of certificates:**

- JKS Keystore file (.jks) (default)  
A Java tool that is called keytool.exe generates the keystore file. The Java Cryptography Extension (.jceks) format requires a specific version of the Java Runtime Environment (JRE). The management server supports only a .jceks keystore file that is generated with the same version as the Java Development Kit on the management server.

---

The keystore file must contain both a certificate and a private key. The keystore password must be the same as the key password. You can locate the password in the following file:

SEPM\_Install\Server Private Key Backup\recovery\_timestamp.zip

SEPM\_Install by default is C:\Program Files\Symantec\Symantec Endpoint Protection Manager.

- PKCS12 keystore file (.pfx and .p12)
  - Certificate and private key file (.der and .pem format)
- Symantec supports unencrypted certificates and private keys in the .der or the .pem format. Pkcs8-encrypted private keys are not supported.

## Best practices for updating server certificates and maintaining the client-server connection

You may need to update the security certificate in the following situations:

- You restore a previous security certificate that the clients already use.
- You want to use a different security certificate than the default certificate (.JKS).

When clients use secure communication with the server, the server certificate is exchanged between the server and the clients. This exchange establishes a trust relationship between the server and clients. When the certificate changes on the server, the trust relationship is broken and clients no longer can communicate. This problem is called orphaning clients.

### NOTE

Use this process to update either one management server or multiple management servers at the same time.

[Steps to update server certificates](#) lists the steps to update the certificate without orphaning the clients that the server manages.

**Table 54: Steps to update server certificates**

Step	Description
Step 1: Break the replication relationship*	If the management server you want to update replicates with other management servers, break the replication relationship. <a href="#">Disabling replication and restoring replication before and after an upgrade</a>
Step 2: Disable server certificate verification	Disable secure communications between the server and the clients. When you disable the verification, the clients stay connected while the server updates the server certificate. <a href="#">Update the server certificate on the management server without breaking communications with the client</a>
Step 3: Wait for all clients to receive the updated policy	The process of deploying the updated policy may take a week or longer, depending on the following factors: <ul style="list-style-type: none"><li>• The number of clients that connect to the management server. Large installations may take several days to complete the process because the managed computers must be online to receive the new policy.</li><li>• Some users may be on vacation with their computers offline.</li></ul> <a href="#">Using the policy serial number to check client-server communication</a>

Step	Description
Step 4: Update the server certificate	<p>Update the server certificate. If you also plan to upgrade the management server, upgrade the certificate first.</p> <p><a href="#">Upgrading a management server</a></p> <p><a href="#">Updating or restoring a server certificate</a></p> <p>You must restart the following services to use the new certificate:</p> <ul style="list-style-type: none"> <li>• The Symantec Endpoint Protection Manager service</li> <li>• The Symantec Endpoint Protection Manager Webserver service</li> <li>• The Symantec Endpoint Protection Manager API service</li> </ul> <p>(As of 14)</p>
Step 5: Enable server certificate verification again	<p>Enable secure communications between the server and the clients again.</p> <p><a href="#">Update the server certificate on the management server without breaking communications with the client</a></p>
Step 6: Wait for all clients to receive the updated policy	The client computers must receive the policy changes from the previous step.
Step 7: Restore the replication relationship*	<p>If the management server you updated replicates with other management servers, restore the replication relationship.</p> <p><a href="#">Disabling replication and restoring replication before and after an upgrade</a></p>

\* You only need to perform these steps if you use replication in your Symantec Endpoint Protection Manager environment.

[Installing Symantec Endpoint Protection Manager](#)

[Generating a new server certificate](#)

## Update the server certificate on the management server without breaking communications with the client

Symantec Endpoint Protection Manager uses a certificate to authenticate communications between it and the Symantec Endpoint Protection clients. The certificate also digitally signs the policy files and installation packages that the client downloads from it. The clients store a cached copy of the certificate in the management server list. If the certificate is corrupted or invalid, the clients cannot communicate with the server. If you disable secure communications, then the clients can still communicate with the server, but do not authenticate communications from the management server.

You disable secure communications to update the certificate in the following situations:

- A site with a single Symantec Endpoint Protection Manager
- A site with more than one Symantec Endpoint Protection Manager, if you cannot enable failover or load balancing

### NOTE

If the certificate is corrupted but otherwise still valid, you can perform disaster recovery as a best practice.

[Disaster recovery best practices for Endpoint Protection](#)

After you update the certificate and the clients check in and receive it, enable secure communications again.

When you update the certificate on a site with multiple management servers and use failover or load balancing, the certificate updates on the management server list. During the process of failover or load balancing, the client receives the updated management server list and the new certificate.

---

## NOTE

Steps 1 through 5 apply only to version 14 and later. If you use 12.x, start with step 6.

1. To update the server certificate on a single management server site without breaking communications with the client, in the console, click **Policies > Policy Components > Management Server Lists**.
2. Under **Tasks**, click **Copy the List**, and then click **Paste List**.
3. Double-click the copy of the list to edit it, and then make the following changes:
  - Click **Use HTTP protocol**.
  - For each server address under **Management Servers**, click **Edit**, and then click **Customize HTTP port**. Leave it at the default of 8014. If you use a custom port, use it here.
4. Click **OK**, and then click **OK** again.
5. Right-click the copy of the list, and then click **Assign**.
6. On the console, click **Clients > Policies > General**.
7. On the **Security Settings** tab, uncheck **Enable secure communications between the management server and clients by using digital certificates for authentication**, and then click **OK**.
8. Wait at least three heartbeat cycles after making this change on all groups before you move to step 9.  
Make sure that you also configure this setting for the groups that do not inherit from a parent group.
9. Update the server certificate.

### [Updating or restoring a server certificate](#)

10. Click **OK**.

To reenable the original settings, wait at least three heartbeat cycles, recheck **Enable secure communications between the management server and clients by using digital certificates for authentication**, and then reassign the original management server list back to your groups.

11. To update the server certificate on a multi-management server site without breaking communications with the client, in the console, ensure that your clients are configured to load balance or failover to at least one other Symantec Endpoint Protection Manager.

### [Setting up failover and load balancing](#)

If you cannot enable load balancing or failover, use the single management server site procedure to first disable then reenable secure communications.

## WARNING

Due to a change in the communication module, client versions 14.2.x cannot use this method to update the server certificate. To avoid breaking communication with these clients, use the single management server site procedure for these client versions, even for multi-management server sites.

12. Update the server certificate on Symantec Endpoint Protection Manager.

### [Updating or restoring a server certificate](#)

13. Wait at least three heartbeat cycles, and then update the server certificate on the next Symantec Endpoint Protection Manager on the site.
14. Repeat steps 2 and 3 until each Symantec Endpoint Protection Manager on the site has the new certificate.

## NOTE

Users who are out of the office or on leave may not receive these updates on their device because it is offline. Many institutions run the failover method for 30 days or more to catch as many out-of-office clients as

---

possible. You may want to leave one Symantec Endpoint Protection Manager running for 90 days with the old certificate to ensure that those users are not orphaned.

[About server certificates](#)

[Best practices for updating server certificates and maintaining the client-server connection](#)

## Updating or restoring a server certificate

The server certificate encrypts and decrypts files between the server and the client. The client connects to the server with an encryption key, downloads a file, and then decrypts the key to verify its authenticity. If you change the certificate on the server without manually updating the client, the encrypted connection between the server and the client breaks.

You must update the server certificate in the following situations:

- You reinstall Symantec Endpoint Protection Manager without using the recovery file. You update the certificate to restore a previous certificate that clients already use.  
[Installing Symantec Endpoint Protection Manager](#)
- You replace one management server with another management server and use the same IP and server name.
- You apply the wrong server certificate (.JKS) after disaster recovery.
- You purchased a different certificate and want to use that certificate instead of the default .JKS certificate.

[About server certificates](#)

[Best practices for updating server certificates and maintaining the client-server connection](#)

To update or restore a server certificate

1. In the console, click **Admin**, and then click **Servers**.
2. Under **Servers**, under **Local Site**, click the management server for which you want to update the server certificate.
3. Under **Tasks**, click **Manage Server Certificate**, and then click **Next**.
4. In the **Manage Server Certificate** panel, click **Update the server certificate**, click **Next**, and then click **Yes**.

To maintain the server-client connection, disable secure connections.

[Update the server certificate on the management server without breaking communications with the client](#)

5. In the **Update Server Certificate** panel, choose the certificate you want to update to, and then click **Next**.
6. For each certificate type, following the instructions on the panels, and click **Finish**.

Backup server certificates are in SEPM\_Install\Server Private Key Backup\recovery\_timestamp.zip. You can locate the password for the keystore file in the settings.properties file within the same .zip file. The password appears in the keystore.password= line.

SEPM\_Install by default is C:\Program Files\Symantec\Symantec Endpoint Protection Manager.

7. You must restart the following services to use the new certificate:
  - The Symantec Endpoint Protection Manager service
  - The Symantec Endpoint Protection Manager Webserver service
  - The Symantec Endpoint Protection Manager API service (As of 14)

[Stopping and starting the management server service](#)

[Stopping and starting the Apache Web server](#)



---

## Reconfiguring Symantec Endpoint Protection Manager after changing the computer's IP address and host name

The Symantec Endpoint Protection (SEP) clients use the host name and IP address of the Symantec Endpoint Protection Manager (SEPM) computer to communicate with SEPM. If you change the computer's host name and the IP address, the clients do not automatically maintain communication. In addition, the SEPM cannot connect to the database because the database server's name is changed and its previous certificate with old computer name and IP address is not valid.

The SEPM web console displays a certificate error because the SEPM computer's IP address and host name are different from the certificate's.

### NOTE

You perform these tasks when SEPM and SEP clients communicate over HTTPS only, and not HTTP.

### To reconfigure Symantec Endpoint Protection Manager and generate a certificate for the SQL Server Express or SQL Server databases:

1. In the Symantec Endpoint Protection Manager, update the management server list to use both the current and the new host name and IP address, and make sure it is assigned to all clients.

The updated list allows SEP client to continue to communicate with SEPM after hostname and IP address changes.

[Assigning a management server list to a group and location](#)

2. On the **Clients > Policies** tab, click the **General > Security Settings** tab, and clear **Enable secure communications between the management server and clients by using digital certificates for authentication**. Disabling secure communications allows the clients to still communicate with the SEPM without needing to authenticate communications with the SEPM.

[Update the server certificate on the management server without breaking communications with the client](#)

3. On the **Clients > Clients** tab, check that the clients are still connected to the management server.
4. Change the SEPM computer IP address.
5. Change the SEPM computer host name, and then restart the SEPM computer.

### NOTE

You can rename just the computer host name and not necessarily the IP address.

6. Stop the SEPM services by running the following commands: `net stop semsrv`, `net stop semapisrv`, and `net stop semwebsrv`.

[Stopping and starting the management server service](#)

7. In the following files:

`<Symantec Endpoint Protection Manager installation directory>\tomcat\conf\Catalina\localhost\root.xml`

`<Symantec Endpoint Protection Manager installation directory>\tomcat\instances\sepm-api\conf\Catalina_WS\localhost\jdbc.properties`

- a. Change `jdbc:sqlserver://SEPM_OLD_COMPUTER_NAME:2638` to `jdbc:sqlserver://SEPM_NEW_COMPUTER_NAME:2638`. If you use a different port number than 2638, continue to use the other number.

- b. Change `trustServerCertificate = false` to `trustServerCertificate = true`

8. Restart the SEPM service by running the following commands: `net start semsrv`, `net start semapisrv`, and `net start semwebsrv`.

9. Log on to SEPM.

If the **Failed to connect to the server** message appears, click **OK** and log on anyway.

10. Generate a new SEPM server certificate.

This step matches the SEPM-to-SEP client certificate information with the new computer name and IP address.

[Generating a new server certificate](#)

11. Log off the SEPM console.

---

12. Do one of the following steps:

Microsoft SQL Server Express database	<ol style="list-style-type: none"><li>1. Reconfigure SEPM. <a href="#">Reinstalling or reconfiguring Symantec Endpoint Protection Manager</a></li><li>2. Log on to SEPM.</li></ol>
Microsoft SQL Server database	<ol style="list-style-type: none"><li>1. Reconfigure SEPM. The TLS message appears.</li><li>2. Generate and import a new SQL TLS certificate. Complete the configuration.</li><li>3. Log on to SEPM.</li></ol> <p>If the SQL Server database is on the same computer as SEPM, see: <a href="#">Reconnecting the Microsoft SQL Server database to the clients after changing the computer's host name</a></p>
Embedded database	Log on to SEPM.

13. Enable **Enable secure communications between the management server and clients by using digital certificates for authentication**.

14. Check that the clients are still connected to SEPM.

[Best practices for updating server certificates and maintaining the client-server connection](#)

### **Reconnecting the Microsoft SQL Server database to the clients after changing the computer's host name**

If you use the Microsoft SQL Server as the database server on the same computer as SEPM, the server name used for ODBC connections changes after you change the computer's host name. You must update the server name that used for ODBC connections. You only change the computer name of SEPM and not the IP address.

**To change the server name that ODBC connections uses:**

1. On the Symantec Endpoint Protection Manager computer, click **Start > Run**.
2. In the Name field, type either `odbc32.cpl` (32-bit) or `odbcad32.exe` (64-bit) and click **OK**.
3. In the **ODBC Data Source Administrator** dialog box, click the **System DSN** tab.
4. Select **SymantecEndpointSecurityDSN** as the System DSN and click **Configure**.
5. Enter the correct connection destination for the server name, such as `\`, and then click **Next**.
6. If you use Windows authentication, select **With Integrated Windows authentication**. If you use SQL server authentication, check **With SQL Server authentication using a login ID and password entered** and input Login ID and password. check **Connect to SQL Server to obtain default settings for the additional configuration options**, and then click **Next**.
7. Select **Change the default database to:**, select **sem5**, and then click **Next**.
8. Click **Finish**.
9. On the ODBC Microsoft SQL Server dialog, click **Test Data Source**.  
If you see the message `TEST COMPLETED SUCCESSFULLY!`, the ODBC connection test is finished.

## **Checking whether the client is connected to the management server and is protected**

After you install the client, check whether the clients are online and connected to the Symantec Endpoint Protection Manager. You can check the connection status on both the console and on the client.

1. To check the client-management server connection on the Symantec Endpoint Protection client, on the client computer, do one of the following tasks:
  - The client shield in the computer's taskbar has a green dot:



- Open the client and look on the Status screen, which states that **Your computer is protected** and displays a green check mark:



- Open the client and click **Help > Troubleshooting**.

#### Symantec Endpoint Protection client status icons

2. To check the client-management server connection in Symantec Endpoint Protection Manager, in the console, click **Clients** and select the target group.
3. On the **Clients** tab, clients that are connected display an icon with a green dot in the **Name** column and display a health state of **Online**:



#### NOTE

Clients that connect through Symantec Endpoint Protection Manager may not immediately display the correct online status in the cloud console. Allow for 5-10 minutes after the online status changes to see an accurate reflection of the current status.

**Table 55: Client status icons in the management console on the Clients > Clients tab > Name column**

Icon	Description
	The client software installation failed.
	<ul style="list-style-type: none"><li>• The client can communicate with Symantec Endpoint Protection Manager. The health state is <b>Online</b>.</li><li>• The client is in computer mode.</li></ul>
	<ul style="list-style-type: none"><li>• The client cannot communicate with Symantec Endpoint Protection Manager. The health state is <b>Offline</b>.</li><li>• The client is in computer mode.</li><li>• The client may have been added from the console, and may not have any Symantec client software installed.</li></ul>
	<ul style="list-style-type: none"><li>• The client can communicate with Symantec Endpoint Protection Manager.</li><li>• The client is in computer mode.</li><li>• The client is an unmanaged detector.</li></ul>
	<ul style="list-style-type: none"><li>• The client cannot communicate with Symantec Endpoint Protection Manager.</li><li>• The client is in computer mode.</li><li>• The client is an unmanaged detector.</li></ul>
	<ul style="list-style-type: none"><li>• The client can communicate with Symantec Endpoint Protection Manager.</li><li>• The client is in user mode.</li></ul>
	<ul style="list-style-type: none"><li>• The client cannot communicate with Symantec Endpoint Protection Manager.</li><li>• The client is in user mode.</li><li>• The client may have been added from the console, and may not have any Symantec client software installed.</li></ul>
	<ul style="list-style-type: none"><li>• The client can communicate with Symantec Endpoint Protection Manager at another site.</li><li>• The client is in computer mode.</li></ul>
	<ul style="list-style-type: none"><li>• The client can communicate with Symantec Endpoint Protection Manager at another site.</li><li>• The client is in computer mode.</li><li>• The client is an unmanaged detector.</li></ul>
	<ul style="list-style-type: none"><li>• The client can communicate with Symantec Endpoint Protection Manager at another site.</li><li>• The client is in user mode</li></ul>

## Symantec Endpoint Protection client status icons





You can check the notification area icon on the client to determine whether the client is connected to a management server and adequately protected. The notification area icon is sometimes referred to as the system tray icon.

The icon is located in the lower-right hand corner of the client computer desktop. You can also right-click this icon to display frequently used commands.

### NOTE

On managed clients, the notification area icon does not appear if the administrator has configured it to be unavailable.

**Table 56: Client status icons**

Icon	Description
	The client runs with no problems. It is either offline or unmanaged. Unmanaged clients are not connected to a management server.
	The client runs with no problems. It is connected to and communicates with the server. All components of the security policy protect the computer.
	The client has a minor problem. For example, the virus definitions may be out of date.
	The client does not run, has a major problem, has an expired license, or has at least one protection technology disabled.

### Hiding and displaying the notification area icon on the Symantec Endpoint Protection client

## Using the policy serial number to check client-server communication

To check whether the server and client communicate, check the policy serial number on the console and on the client. If the client communicates with the management server and receives regular policy updates, the serial numbers should match.

If the policy serial numbers do not match, you can try to manually update the policies on the client computer and check the troubleshooting logs.

### Updating client policies

#### Updating policies and content on the client using push mode or pull mode

1. **Option 1:** To view the policy serial number in the console, in the console, click **Clients**.
2. Under **Clients**, select the relevant group.

The policy serial number and policy date appear in the upper right corner of the program window.

### NOTE

The policy serial number and the policy date also appear at the bottom of the details list on the **Details** tab.

3. **Option 2:** To view the policy serial number on the client computer, on the client computer, in the client, click **Help > Troubleshooting**.

On the **Management** tab, look at the policy serial number.

The serial number should match the serial number on the console for the group that the client computer is in.

### Performing the tasks that are common to all policies

---

## Updating policies and content on the client using push mode or pull mode

[Deciding whether to use pull mode or push mode to connect between Symantec Endpoint Protection Manager and the clients](#)

[Configuring push mode or pull mode for a group](#)

### Deciding whether to use pull mode or push mode to connect between Symantec Endpoint Protection Manager and the clients

When you configure policies on the management server, you need to have the updated policies downloaded to the client computers. In the console, you can configure client computers to use either of the following update methods:

Pull mode	The client computer connects to the management server periodically, depending on the frequency of the heartbeat setting. The client computer checks the status of the management server when the client connects.
Push mode	The client computer establishes a constant HTTP connection to the management server. Whenever a change occurs in the management server status, it notifies the client computer immediately.

In either mode, the client computer takes the corresponding action, based on the change in the status of the management server. Because it requires a constant connection, push mode requires a large amount of network bandwidth. Client computers that are configured to use pull mode require less bandwidth.

The heartbeat protocol defines the frequency at which client computers upload data such as log entries and download policies. The first heartbeat occurs immediately after the client starts. The next heartbeat occurs at the heartbeat frequency that you set.

The heartbeat frequency is a key factor in the number of clients that each Symantec Endpoint Protection Manager can support. If you set a heartbeat frequency to 30 minutes or less, it limits the total number of clients that Symantec Endpoint Protection Manager can support. For deployments of 1,000 clients or more, Symantec recommends that you set the heartbeat frequency to the maximum length of time possible. Symantec recommends that you use the longest interval that still meets your company's security requirements. For example, if you want to update policies and gather logs on a daily basis, then you might set the heartbeat frequency to 24 hours. Assess the proper configuration, hardware, and network architecture necessary for your network environment.

#### NOTE

You can also update policies manually on a client computer.

[Using the policy serial number to check client-server communication](#)

[Communication ports for Symantec Endpoint Protection](#)

### Configuring push mode or pull mode for a group

You can specify whether Symantec Endpoint Protection Manager pushes the policy down to the clients or that the clients pull the policy from Symantec Endpoint Protection Manager. The default setting is push mode. If you select pull mode, then by default, clients connect to the management server every 5 minutes, but you can change this default heartbeat interval.

[Performing the tasks that are common to all policies](#)

---

You can set the mode for a group or for a location.

1. To configure push mode or pull mode for a group, in the console, click **Clients**.
2. Under **Clients**, select the group for which you want to specify whether to push or pull policies.
3. Click **Policies**.
4. Uncheck **Inherit policies and setting from the parent group "group name"**.
5. Under **Location-independent Policies and Settings** pane, under **Settings**, click **Communications Settings**.
6. In the **Communications Settings for group name** dialog box, under **Download**, verify that **Download policies and content from the management server** is checked.
7. Do one of the following tasks:
  - Click **Push mode**.
  - Click **Pull mode** and under **Heartbeat Interval**, set the number of minutes or hours.
8. Click **OK**.
9. To specify push mode or pull mode for a location, in the console, click **Clients**.
10. Under **Clients**, select the group for which you want to specify whether to push or pull policies.
11. Click **Policies**.
12. Uncheck **Inherit policies and setting from the parent group "group name"**.
13. Under **Location-specific Policies and Settings**, under **Location-specific Policies** for the location you want to modify, expand **Location-specific Settings**.
14. Under **Location-specific Settings**, to the right of **Communications Settings**, click **Tasks** and uncheck **Use Group Communications Settings**.
15. To the right of **Communications Settings**, click **Local - Push** or **(Local - Pull)**.
16. Do one of the following tasks:
  - Click **Push mode**.
  - Click **Pull mode** and under **Heartbeat Interval**, set the number of minutes or hours.
17. Click **OK**.

[Performing the tasks that are common to all policies](#)

## How does the client computer and the management server communicate?

Symantec Endpoint Protection Manager connects to the client with a communications file called Sylink.xml. The Sylink.xml file includes the communication settings such as the IP address of the management server and the heartbeat interval. After you install a client installation package on to the client computers, the client and the server automatically communicate.

The sylink file performs many of its functions during the heartbeat. The heartbeat is the frequency at which client computers upload logs to the management server, and download policies and commands.

The sylink file contains:

- The public certificate for all management servers.
- The KCS, or encryption key.
- The Domain ID that each client belongs to.

---

## NOTE

Do not edit the sylink file. If you change the settings, the management server overwrites most settings the next time the client connects to the management server.

[Updating policies and content on the client using push mode or pull mode](#)

## Troubleshooting Sylink communication

In version 14.2, the communications module was upgraded, and includes new log files. You can use this information to troubleshoot communication issues between Symantec Endpoint Protection Manager and the clients.

The 14.2 communications module works with all client types, including Windows, Mac, and Linux, and has improved IPv6 support.

## NOTE

As of version 14.2, the communication module only honors system proxy information.

1. To view the log files for the communications module, on the Windows client, in the following folder:

```
C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data
```

You can view the following files:

- **For client registration:**

- `RegistrationInfo.xml`

- Client registration metadata that the client submits to Symantec Endpoint Protection Manager.

- `Registration.xml`

- Client registration metadata that Symantec Endpoint Protection Manager returns to the client.

- `State.xml`

- Includes internal settings, such as the management server IP address.

- **For the communications module logs:**

- `\Logs\cve.log` and `\Logs\cve-actions.log`

- Use these logs to troubleshoot communication between Symantec Endpoint Protection Manager and the client.

- Send these logs to Technical Support if asked.

- **For the opstate status:**

- Appears in the logs in the `\Pending` and `\Sent` folders

2. To configure the communication module logs, open the Windows Registry Editor, click **Start > Run**, type `regedit`, and then click **OK**.

3. To enable the `cve.log` or `cve-actions.log`, open the following Windows registry key:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink  
REG_DWORD: CVELogLevel
```

Use any of the following values:

- 1 = Debug
- 2 = Info
- 3 = Warning
- 4 = Error
- 5 = Fatal

If the registry key is not present or does not have a valid value, it defaults to 4. The installation default is also 4.

For example, you can type:

---

**32-bit:** [HKLM\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink]  
"CVELogLevel"=dword:00000001

**64-bit:** [HKLM\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink] "CVELogLevel"=dword:00000001

4. To control the size of these logs, use the following registry value: [HKEY\_LOCAL\_MACHINE\SOFTWARE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink] REG\_DWORD: CVELogSizeDB

The default size is 250 MB.

[How to enable Communication Module logging in Endpoint Protection 14.2](#)

[How to enable Sylink debugging for Endpoint Protection clients \(14.1 and earlier\)](#)

## How do I replace the client-server communications file on the client computer?

### When should I replace the client-server communications file on the client computer?

Normally you do not need to replace the Sylink.xml file. However, you may need to replace the existing Sylink.xml file on the client computer in the following situations:

- The client and the server do not communicate. If the clients have lost the communication with the management server, you must replace the old Sylink.xml file with a new file.  
[Checking the connection to the management server on the client computer](#)
- You want to convert an unmanaged client to a managed client. If a user installs a client from the installation file, the client is unmanaged and does not communicate with the management server. You can also reinstall the client software on the computer as a managed computer.  
[About managed and unmanaged clients](#)
- You want to manage a previously orphaned client. For example, if the hard drive that the management server is installed on gets corrupted, you must reinstall the management server. You can update the Sylink.xml file on the orphaned clients to re-establish communication with them.  
[Update the server certificate on the management server without breaking communications with the client](#)  
[Exporting the client-server communications file \(Sylink.xml\) manually](#)
- You want to move a large number of clients from multiple groups to a single group. For example, you might want to move the client computers in a remote group and a laptop group to a test group. Typically, you need to move the client computers one group at a time.  
[Moving a client computer to another group](#)

[How do I replace the client-server communications file on the client computer?](#)

[Restoring client-server communications with Communication Update Package Deployment](#)

[How to convert an unmanaged Symantec Endpoint Protection for Macintosh client to managed](#)

### How do I replace the client-server communications file on the client computer?

**If you need to replace the client-server communications file (Sylink.xml) on the client computer, you can use the following methods:**

- Create a new client installation package and deploy it on the client computers. Use this method if manually importing the Sylink.xml on large environment is physically not possible and requires administrative access.  
[Restoring client-server communications with Communication Update Package Deployment](#)
- Write a script that runs the SylinkDrop tool, which is located in the \Tools folder of the installation file. Symantec recommends this method for a large number of clients. You should also use the SylinkDrop tool if you use a software



management tool to download the client software to computers. The advantage of the software management tool is that it downloads the Sylink.xml file as soon as the end user turns on the client computer. In comparison, the client installation package downloads the new Sylink.xml file only after the client computer connects to the management server.

[Restoring client-server communication settings by using the SylinkDrop tool](#)

- Export the Sylink.xml file to the client computer and import it on the client computer manually. Symantec recommends this method if you want to use a software management tool. With a software management tool, the job is queued up and completed whenever the users turn on their computer. With the other methods, the client computer must be online.

[Steps for exporting and importing the communications file](#) displays the process for exporting and importing the Sylink.xml file into the client computer.

**Table 57: Steps for exporting and importing the communications file**

Step	Description
Step 1: Export a file that includes all the communication settings for the group that you want the client to be in.	The default file name is group_name_sylink.xml. <a href="#">Exporting the client-server communications file (Sylink.xml) manually</a>
Step 2: Deploy the file to the client computer.	You can either save the file to a network location or send it to an individual user on the client computer.
Step 3: Import the file on the client computer.	Either you or the user can import the file on the client computer. <a href="#">Importing client-server communication settings into the Windows client</a> Unmanaged clients are not password-protected, so you do not need a password on the client. However, if you try to import a file into a managed client that is password-protected, then you must enter a password. The password is the same one that is used to import or export a policy. <a href="#">Password-protecting the Symantec Endpoint Protection client</a> You do not need to restart the client computer.
Step 4: Verify client and server communication on the client.	The client immediately connects to the management server. The management server places the client in the group that is specified in the communication file. The client is updated with the group's policies and settings. After the client and the management server communicate, the notification area icon with the green dot appears in the client computer's taskbar. <a href="#">Checking whether the client is connected to the management server and is protected</a>

[Client and server communication files](#)

[How does the client computer and the management server communicate?](#)

## Restoring client-server communications with Communication Update Package Deployment

If the client-server communications break, you can quickly restore communications by replacing the Sylink.xml file on the client computer. You can replace the Sylink.xml file by deploying a communication update package. Use this method for a large number of computers, for the computers that you cannot physically access easily, or the computers that require administrative access.

[How does the client computer and the management server communicate?](#)

[How do I replace the client-server communications file on the client computer?](#)

1. In the console, launch the **Client Deployment Wizard**.

Click **Help > Getting Started Page** and then under **Required tasks**, click **Install the client software on your computers**.

---

2. In the **Client Deployment Wizard**, under **Communication Update Package Deployment**, select whether you want a package for Windows or Mac clients, and then click **Next**.

3. Select the group on which you want to apply the policy, and then click **Next**.

For Windows clients only, you can set password protection.

[Password-protecting the Symantec Endpoint Protection client](#)

4. Choose one of the following deployment methods, and then click **Next**:

- Click **Remote Push** and go to the **Computer Selection** step in the following procedure.

[Installing Symantec Endpoint Protection clients with Remote Push](#)

- **Save Package** and go to the **Browse** step in the following procedure.

[Installing Symantec Endpoint Protection clients with Save Package](#)

5. After the communication update package is applied, confirm that the computers successfully communicate with Symantec Endpoint Protection Manager.

[Checking whether the client is connected to the management server and is protected](#)

[Running a report on the deployment status of clients](#)

## Exporting the client-server communications file (Sylink.xml) manually

If the client and the server do not communicate, you may need to replace the Sylink.xml file on the client computer to restore communications. You can manually export the Sylink.xml file from Symantec Endpoint Protection Manager on a group basis.

The most common reasons for replacing the Sylink.xml on the client are:

- To convert an unmanaged client into a managed client.
- To reconnect a previously orphaned client to the management server.

[Update the server certificate on the management server without breaking communications with the client](#)

[How does the client computer and the management server communicate?](#)

If you need to update client-server communications for a large number of clients, deploy the Communication Update Package instead of using this method.

[Restoring client-server communications with Communication Update Package Deployment](#)

1. In the console, click **Clients**.

2. Under **Clients**, select the group in which you want the client to appear.

3. Right-click the group, and then click **Export Communication Settings**.

4. In the **Export Communication Settings for group name** dialog box, click **Browse**.

5. In the **Select Export File** dialog box, locate the folder to where you want to export the .xml file, and then click **OK**.

6. Under **Preferred Policy Mode**, make sure that **Computer Mode** is checked.

7. Click **Export**.

If the file name already exists, click **OK** to overwrite it or **Cancel** to save the file with a new file name.

To finish the conversion, you or a user must import the communications setting on the client computer.

[Importing client-server communication settings into the Windows client](#)

---

## Importing client-server communication settings into the Windows client

Once you have exported client-server communication settings, you can import them into a Windows client. You can use it to convert an unmanaged client into a managed client or to reconnect a previously orphaned client with Symantec Endpoint Protection Manager.

To import the client-server communications settings file into the Windows client

1. Open Symantec Endpoint Protection on the computer that you want to convert to a managed client.
2. In the upper right, click **Help**, and then click **Troubleshooting**.
3. In the **Troubleshooting** dialog box, in the **Management** pane, click **Import**.
4. In the **Import Group Registration Settings** dialog box, locate the group name\_sylink.xml file, and then click **Open**.
5. Click **Close** to close the **Troubleshooting** dialog box.

After you import the communications file, and the client and the management server communicate, the notification area icon appears with a green dot in the computer's taskbar. The green dot indicates that the client and the management server are in communication with each other.

[Exporting the client-server communications file \(Sylink.xml\) manually](#)

[Restoring client-server communications with Communication Update Package Deployment](#)

## Importing client-server communication settings into the Linux client

(For 14.3 MP1 and earlier)

After you install an unmanaged Symantec Endpoint Protection for Linux client, you can convert it to a managed client to centrally manage the client's policies and status with Symantec Endpoint Protection Manager. A managed client communicates with and reports its status and other information to Symantec Endpoint Protection Manager.

You can also use this procedure to reconnect a previously orphaned client with Symantec Endpoint Protection Manager.

### NOTE

You must have superuser privileges to perform this procedure. The procedure uses `sudo` to demonstrate this elevation of privilege as required.

The text path-to-sav represents the path to the sav command. The default path is `/opt/Symantec/symantec_antivirus/`.

### To import the client-server communication settings file into the Linux client:

1. You or the Symantec Endpoint Protection Manager administrator must first export the communication settings file from Symantec Endpoint Protection Manager and copy it to the Linux computer. Ensure that the file name is `sylink.xml`.

[Exporting the client-server communications file \(Sylink.xml\) manually](#)

2. On the Linux computer, open a terminal window and enter the following command:

```
sudo path-to-sav/sav manage -i path-to-sylink/sylink.xml
```

Where path-to-sylink represents the path to which you copied `sylink.xml`.

For example, if you copied it to your user profile's desktop, enter:

```
sudo path-to-sav/sav manage -i ~/Desktop/sylink.xml
```

- 
3. A successful import returns OK. To further verify the managed status, enter the following command, which displays the policy serial number for a successful import:

```
path-to-sav/sav manage -p
```

### Installing the Symantec Endpoint Protection client for Linux

#### NOTE

As of Linux client 14.3 RU2, you can use the **sav** command to import the *sylink.xml* file.

For more information, see [Running the Linux client command line tool \(sav\)](#).

## IPv6 networking support

This support was added in version 14.2.

IPv6 is a revision to the Internet Protocol that is a successor of IPv4. Both types of addresses provide the unique, numerical IP addresses necessary for Internet-enabled devices to communicate. IPv4 addresses are 32-bit, and IPv6 addresses are 128-bit. Therefore, IPv6 allows for more addresses to be available for users and devices to communicate on the Internet.

IPv6 addresses are conventionally expressed using hexadecimal strings. For example,

`fd32:32a4:d0cf:a0c4:0000:8a2e:0370:7334`, which can also be expressed as

`fd32:32a4:d0cf:a0c4::8a2e:0370:7334`. When you enter an IPv6 address that ends in a port number, you must enclose the IPv6 address in square brackets. The brackets keep the port number from being interpreted as part of the IPv6 address. For example: `http://[fd32:32a4:d0cf:a0c4::8a2e:0370:7334]:9090`.

Symantec Endpoint Protection 14.2 supports IPv6 in the following ways:

- Communication between the management server and Windows, Mac, and Linux clients
- Communication between the console and the management server, such as logging on locally or remotely to Symantec Endpoint Protection Manager
  - [Logging on to the Symantec Endpoint Protection Manager console](#)
- Communication between management servers and internal LiveUpdate servers that run LiveUpdate Administrator.
  - [Configuring clients to download content from an internal LiveUpdate server](#)
- Windows LiveUpdate to management server
- Communication between management server or clients and services or functions like LiveUpdate Engine (LUE) and reputation look-ups
- Definition of locations in Location Awareness with IPv6-based criteria

Furthermore, many other policies now let you enter IPv6 addresses as defining criteria in addition to IPv4, such as custom IPS signatures or explicit GUPs.

IPv6 is not supported for the following items:

- Two-factor authentication (2FA) with Symantec VIP
  - [Configuring two-factor authentication with Symantec VIP](#)
- Enrolling with and connecting to the cloud console

---

# Managing Groups, Clients, Administrators, and Domains

---

Learn how to add and manage groups, clients, administrators, passwords, and domains

This section describes how to manage groups of client computers, clients, administrators, passwords, and domains.

## Managing groups of clients

In Symantec Endpoint Protection Manager, groups function as containers for the endpoints that run the client software. These endpoints can be either computers, or users. You organize the clients that have similar security needs into groups to make it easier to manage network security.

**Symantec Endpoint Protection Manager contains the following default groups:**

- The **My Company** group is the top-level, or parent, group. It contains a flat tree of child groups.
- The **Default Group** is a subgroup of **My Company**. Clients are first assigned to the **Default Group** when they first register with Symantec Endpoint Protection Manager, unless they belong to a predefined group. You cannot create subgroups under the **Default Group**.

### NOTE

You cannot rename or delete the default groups.

If you rename **My Company** in the cloud console, the group name does not change in Symantec Endpoint Protection Manager.

**Table 58: Group management actions**

Task	Description
Add groups	<a href="#">How you can structure groups</a> <a href="#">Adding a group</a>
Import existing groups	If your organization already has an existing group structure, you can import the groups as organizational units.  <b>Note:</b> You cannot manage imported organizational units in the same ways that you can manage the groups that you create in Symantec Endpoint Protection Manager.  <a href="#">Importing existing groups and computers from an Active Directory or an LDAP server</a>
Disable inheritance for subgroups	The subgroups inherit the same security settings from the parent group by default. You can disable inheritance. <a href="#">Disabling a group's inheritance</a>
Create locations within groups	You can set up the clients to switch automatically to a different security policy if the physical location of the client changes. <a href="#">Managing locations for remote clients</a> Some security settings are group-specific and some settings are location-specific. You can customize any settings that are location-specific. <a href="#">Configuring communication settings for a location</a>
Manage security policies for groups	You can create security policies based on the needs of each group. You can then assign different policies to different groups or locations. <a href="#">Adding a policy</a> <a href="#">Assigning a policy to a group or location</a> <a href="#">Performing the tasks that are common to all policies</a>

Task	Description
Perform group maintenance	You can move groups for easier management and move clients between groups. You can also block clients from being added to a particular group. <a href="#">Moving a client computer to another group</a> <a href="#">Blocking client computers from being added to groups</a>

## How you can structure groups

You can create multiple groups and subgroups to match the organizational structure and security of your company. You can base your group structure on function, role, geography, or a combination of criteria.

**Table 59: Criteria for creating groups**

Criterion	Description
Function	You can create groups based on the types of computers to be managed, such as laptops, desktops, and servers. Alternatively, you can create multiple groups that are based on usage type. For example, you can create a remote group for the client computers that travel and a local group for the client computers that remain in the office.
Role	You can create groups for department roles, such sales, engineering, finance, and marketing.
Geography	You can create groups based on the offices, cities, states, regions, or countries where the computers are located.
Combination	You can create groups based on a combination of criteria. For example, you can use the function and the role. <b>You can add a parent group by role and add child subgroups by function, as in the following scenario:</b> <ul style="list-style-type: none"> <li>Sales, with subgroups of laptops, desktops, and servers.</li> <li>Engineering, with subgroups of laptops, desktops, and servers.</li> </ul>

After you organize the client computers into groups, you can apply the appropriate amount of security to that group.

For example, suppose that a company has telemarketing and accounting departments. These departments have staff in the company's New York, London, and Frankfurt offices. All computers in both departments are assigned to the same group so that they receive virus and security risk definitions updates from the same source. However, IT reports indicate that the telemarketing department is more vulnerable to risks than the accounting department. As a result, the system administrator creates separate telemarketing and accounting groups. Telemarketing clients share configuration settings that strictly limit how users can interact with their virus and security risk protection.

### [Best Practices for Creating Group Structure](#)

#### [Performing the tasks that are common to all policies](#)

#### [Managing groups of clients](#)

## Adding a group

You can add groups after you define the group structure for your organization.

Group descriptions may be up to 1024 characters long. Group names may contain any character except the following characters: " / \ \* ? < > | : Group descriptions are not restricted.

### NOTE

You cannot add groups to the Default Group.

### [How you can structure groups](#)

To add a group

1. In the console, click **Clients**.
2. Under **Clients**, select the group to which you want to add a new subgroup.
3. On the **Clients** tab, under **Tasks**, click **Add Group**.
4. In the **Add Group for group name** dialog box, type the group name and a description.
5. Click **OK**.

## Importing existing groups and computers from an Active Directory or an LDAP server

If your company uses either Active Directory or an LDAP server to manage groups, you can import the group structure into Symantec Endpoint Protection Manager. You can then manage the groups and computers from the management console.

[Importing existing groups and computers](#) lists the tasks you should perform to import the group structure before you can manage them.

**Table 60: Importing existing groups and computers**

Step	Description
Step 1: Connect Symantec Endpoint Protection Manager to your company's directory server	You can connect Symantec Endpoint Protection Manager to either Active Directory or an LDAP-compatible server. When you add the server, you should enable synchronization. <a href="#">About importing organizational units from the directory server</a> <a href="#">Connecting Symantec Endpoint Protection Manager to a directory server</a> <a href="#">Connecting to a directory server on a replicated site</a>
Step 2: Import either entire organizational units or containers	You can import the existing group structure from Active Directory or LDAP into the Symantec Endpoint Protection Manager. You can also copy individual accounts from an imported group structure into an existing Symantec Endpoint Protection Manager group structure. <a href="#">Importing organizational units from a directory server</a>
Step 3: Either keep imported computer or user accounts in their own group or copy imported accounts to existing groups	After you import organizational units, you can do either of the following actions: <ul style="list-style-type: none"> <li>• Keep the imported organizational units or accounts in their own groups. After you import organizational units or individual accounts, you assign policies to the organizational unit or group.</li> <li>• Copy the imported accounts to existing Symantec Endpoint Protection Manager groups. The copied accounts follow the policy of the Symantec Endpoint Protection Manager group and not the imported organizational unit.</li> </ul> <a href="#">Adding a group</a> <a href="#">Assigning a policy to a group or location</a> <a href="#">The types of security policies</a>
Step 4: Change the authentication method for administrator accounts (optional)	For the administrator accounts that you added in Symantec Endpoint Protection Manager, change the authentication method to use directory server authentication instead of the default Symantec Endpoint Protection Manager authentication. You can use the administrator accounts to authenticate the accounts that you imported. When an administrator logs on to Symantec Endpoint Protection Manager, the management server retrieves the user name from the database and the password from the directory server. <a href="#">Choosing the authentication method for administrator accounts</a> <a href="#">Checking the authentication to a directory server</a>

### About importing organizational units from the directory server

Microsoft Active Directory and LDAP servers use organizational units to manage accounts for computers and users. You can import an organizational unit and its account data into Symantec Endpoint Protection Manager, and manage the

---

account data in the management console. Because Symantec Endpoint Protection Manager treats the organizational unit as a group, you can then assign a security policy to the organizational unit group.

You can also move accounts from the organizational units into a Symantec Endpoint Protection Manager group by copying the accounts. The same account then exists in both the Symantec Endpoint Protection Manager group and the organizational unit. Because the priority of the Symantec Endpoint Protection Manager group is higher than the organizational unit, the copied accounts adopt the policy of the Symantec Endpoint Protection Manager group.

If you delete an account from the directory server that you copied to a Symantec Endpoint Protection Manager group, the account name still remains in the Symantec Endpoint Protection Manager group. You must remove the account from the management server manually.

If you need to modify the account data in the organizational unit, you perform this task on the directory server, and not in Symantec Endpoint Protection Manager. For example, you can delete an organizational unit from the management server, which does not permanently delete the organizational unit in the directory server. You must synchronize Symantec Endpoint Protection Manager with the Active Directory server so that these changes get automatically updated in Symantec Endpoint Protection Manager. You enable synchronization when you set up the connection to the directory server.

#### **NOTE**

Synchronization is only possible for Active Directory Servers. Symantec Endpoint Protection does not support synchronization with LDAP servers.

You can also import selected users to a Symantec Endpoint Protection Manager group rather than importing the entire organizational unit.

[Connecting Symantec Endpoint Protection Manager to a directory server](#)

[Importing existing groups and computers from an Active Directory or an LDAP server](#)

[Importing organizational units from a directory server](#)

## **Connecting Symantec Endpoint Protection Manager to a directory server**

You must first connect Symantec Endpoint Protection Manager to your company's directory server before you can import the organizational units that contain computer accounts or user accounts.

You cannot modify the accounts in organizational units in the management server, only in the directory server. However, you can synchronize the account data between an Active Directory server and the management server. Any changes you make in the Active Directory server are automatically updated in Symantec Endpoint Protection Manager. Any changes that you make on the Active Directory server do not appear immediately in the organizational unit that was imported into the management server. The latency period depends on the synchronization frequency. You enable synchronization and set the synchronization frequency when you configure the connection.

If you delete a directory server connection from Symantec Endpoint Protection Manager, you must first delete any organizational units that you imported that are associated with that connection. Then you can synchronize data between the servers.

#### **NOTE**

Synchronization is only possible for Active Directory Servers. Symantec Endpoint Protection does not support synchronization with LDAP servers.

To connect Symantec Endpoint Protection Manager to a directory server



- 
1. In the console, click **Admin > Servers**.
  2. Under **Servers** and **Local Site**, select the management server.
  3. Under **Tasks**, click **Edit the server properties**.
  4. In the **Server Properties** dialog box, on the **Directory Servers** tab, click **Add**.
  5. In the **Add Directory Server** dialog box, type a name for the directory server.
  6. Check **Active Directory** or **LDAP** and type the IP address, host name, or domain name.  
If you add an LDAP server, change the port number of the LDAP server if it should be different than the default value.
  7. If you want an encrypted connection, check **Use Secure Connection**.
  8. Click **OK**.
  9. On the **Directory Servers** tab, check **Synchronize with Directory Servers** and under **Schedule**, set up the synchronization schedule.
  10. Click **OK**.

#### Importing organizational units from a directory server

### Connecting to a directory server on a replicated site

If a site uses a replicated Active Directory or LDAP server, you can connect Symantec Endpoint Protection Manager to both the primary directory server and the replicated server. If the primary directory server gets disconnected, the management server stays connected to the replicated directory server.

Symantec Endpoint Protection Manager can then authenticate administrator accounts and synchronize organizational units on all the Active Directory servers of the local site and the replicated sites.

#### Setting up sites and replication

##### NOTE

Synchronization is only possible for Active Directory Servers. Symantec Endpoint Protection does not support synchronization with LDAP servers.

To connect to a directory server on a replicated site

1. In the console, click **Admin > Servers**.
2. Under **Servers**, select the management server.
3. Under **Tasks**, click **Edit the server properties**.
4. In the **Server Properties** dialog box, on the **Directory Servers** tab, click **Add**.
5. In the **Add Directory Server** dialog box, on the **Replication Servers** tab, click **Add**.
6. In the **Add Replication Server** dialog box, type the IP address, host name, or domain name for the directory server, and then click **OK**.
7. Click **OK**.
8. Click **OK**.

#### Connecting Symantec Endpoint Protection Manager to a directory server

---

## Importing organizational units from a directory server

When you import computer accounts or user accounts from an Active Directory or LDAP server, you import these accounts as organizational units. You can then apply a security policy to the organizational unit. You can also copy these accounts to an existing Symantec Endpoint Protection Manager group.

You can import the organizational unit as a subgroup of either the **My Company** group or a group you create, but not the **Default Group**. You cannot create groups as a subgroup of an organizational unit. You cannot place an organizational unit in more than one Symantec Endpoint Protection Manager group.

If you do not want to add all accounts within an organizational unit or container to Symantec Endpoint Protection Manager, then you must still import it. Once the import completes, you copy the accounts that you want to manage to existing client groups.

### NOTE

Before you import organizational units into Symantec Endpoint Protection Manager, you must convert some of the special characters that precede a computer name or user name. You perform this task in the directory server. If you do not convert special characters, the management server does not import these accounts.

### You must convert the following special characters:

- A space or a hash character (#) that occurs at the beginning of an entry.
- A space character that occurs at the end of an entry.
- A comma (,), plus sign (+), double quotation mark ("), less than or greater than symbols (< or >), equals sign (=), semi-colon (;), backslash (\).

To allow a name that includes these characters to be imported, you must precede each character with a backslash character (\).

To import organizational units from a directory server

1. Connect Symantec Endpoint Protection Manager to a directory server.

[Connecting Symantec Endpoint Protection Manager to a directory server](#)

2. In the console, click **Clients**, and under **Clients**, select the group to which you want to add the organizational unit.
3. Under **Tasks**, click **Import Organizational Unit or Container**.
4. In the **Domain** drop-down list, choose the directory server name you created in step [Connect Symantec Endpoint Protection Manager to a directory server](#).
5. Select either the domain or a subgroup.
6. Click **OK**.

[Importing existing groups and computers from an Active Directory or an LDAP server](#)

[About importing organizational units from the directory server](#)

## Disabling a group's inheritance

In the group structure, subgroups initially and automatically inherit the locations, policies, and settings from their parent group. By default, inheritance is enabled for every group. You can disable inheritance so that you can configure separate security settings for a subgroup. If you make changes and later enable inheritance, any changes that you made in the subgroup's settings are overwritten.

Policies that come from the cloud do not follow the Symantec Endpoint Protection Manager policy inheritance configuration. Instead, they follow the inheritance rules that are defined in the cloud.

[Managing groups of clients](#)

---

To disable a group's inheritance

1. In the console, click **Clients**.
2. On the **Clients** page, under **Clients**, select the group for which you want to disable or enable inheritance.  
You can select any group except the top-level group, My Company.
3. In the **group name** pane, on the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.

## Blocking client computers from being added to groups

You can set up client installation packages with their group membership already defined. If you define a group in the package, the client computer automatically is added to the appropriate group. The client is added the first time it makes a connection to the management server.

### Managing client installation packages

You can block a client if you do not want clients to be added automatically to a specific group when they connect to the network. You can block a new client from being added to the group to which they were assigned in the client installation package. In this case, the client gets added to the default group. You can manually move a computer to a blocked group.

1. In the console, click **Clients**.
2. Under **Clients**, right-click a group, and click **Properties**.
3. On the **Details** tab, under **Tasks**, click **Edit Group Properties**.
4. In the **Group Properties for group name** dialog box, click **Block New Clients**.
5. Click **OK**.

### Moving a client computer to another group

## Moving a client computer to another group

If your client computers are not in the correct group, you can move them to another group.

To move client from multiple groups into a single group, you can redeploy the client installation package.

### Restoring client-server communications with Communication Update Package Deployment

1. In the console, click **Clients**.
2. On the **Clients** page, select a group.
3. On the **Clients** tab, in the selected group, select the computer, and then right-click **Move**.  
Use the Shift key or the Control key to select multiple computers.
4. In the **Move Clients** dialog box, select the new group.
5. Click **OK**.

### Managing groups of clients

# Managing client computers

**Table 61: Tasks to manage client computers**

Task	Description
Check that the client software is installed on your computers	<ul style="list-style-type: none"> <li>You can display the computers in each group that do not have the client software installed yet. <a href="#">Searching for the clients that do not have the client software installed</a></li> <li>You can configure a client computer to detect that other devices do not have the client software installed. Some of these devices might be unprotected computers. You can then install the client software on these computers. <a href="#">Configuring a client to detect unmanaged devices</a></li> <li>You can add a client to a group and install the client software later. <a href="#">Choosing a method to install the client using the Client Deployment Wizard</a></li> </ul>
Check whether the client is connected to the management server	<p>You can check the client status icons in the management console and in the client. The status icon shows whether the client and the server communicate.</p> <p><a href="#">Checking whether the client is connected to the management server and is protected</a></p> <p><a href="#">Symantec Endpoint Protection client status icons</a></p> <p>A computer may have the client software installed, but is an unmanaged client. You cannot manage an unmanaged client. Instead, you can convert the unmanaged client to a managed client.</p> <p><a href="#">How does the client computer and the management server communicate?</a></p>
Configure the connection between the client and the server	<p>After you install the client software client computers automatically connect to the management server at the next heartbeat. You can change how the server communicates with the client computer.</p> <p><a href="#">Managing the client-server connection</a></p> <p>You can troubleshoot any connection issues.</p> <p><a href="#">Troubleshooting communication problems between Symantec Endpoint Protection Manager and the console or the database</a></p>
Check that client computers have the right level of protection	<ul style="list-style-type: none"> <li>You can view the status of each protection technology on your client computers. <a href="#">Viewing the protection status of client computers</a></li> <li>You can run reports or view logs to see whether you need to increase protection or improve performance. For example, the scans may cause false positives. You can also identify the client computers that need protection. <a href="#">Monitoring endpoint protection</a></li> <li>You can modify protection based on specific attributes of the client software or the client computers. <a href="#">Searching for information about client computers</a></li> </ul>
Adjust the protection on client computers	<p><b>If you decide that clients do not have the right level of protection, you can adjust the protection settings.</b></p> <ul style="list-style-type: none"> <li>You can increase or decrease each type of protection based on the results in the reports and logs. <a href="#">The types of security policies</a> <a href="#">How Symantec Endpoint Protection technologies protect your computers</a></li> <li>You can require a password on the client. <a href="#">Password-protecting the Symantec Endpoint Protection client</a></li> </ul>
Move endpoints from one group to another to modify protection (optional)	<p>To change a client computer's level of protection, you can move it to a group that provides more protection or less protection.</p> <p><a href="#">Moving a client computer to another group</a></p> <p>When you deploy a client installation package, you specify which group the client goes in. You can move the client to a different group. But if the client gets deleted or disconnected and then gets added again and reconnected, the client returns to the original group. To keep the client with the group it was last moved to, configure the reconnection preferences. You configure these settings in the <b>Communications Settings</b> dialog box on the <b>Clients &gt; Policies</b> tab.</p> <p><a href="#">Communications Settings for &lt;group_name&gt;</a></p>

Task	Description
Decide whether users should have control over computer protection (optional)	<p>You can specify the kind of control that users have over the protection on client computers.</p> <ul style="list-style-type: none"> <li>For Virus and Spyware Protection, Proactive Threat Protection, and Memory Exploit Mitigation, you can lock or unlock a check box within the policies to specify whether users can change individual settings.</li> <li>For the Firewall policy and the IPS policy and for some client user interface settings, you can change the user control level more generally. <a href="#">Preventing users from disabling protection on client computers</a> </li> <li>If users need full control of the client, you can install an unmanaged client. <a href="#">How does the client computer and the management server communicate?</a> </li> </ul>
Remove the Symantec Endpoint Protection client software from decommissioned computers (optional)	<p>If you decommissioned a client computer and you want to use the license for a different computer, you can uninstall the Symantec Endpoint Protection client software. For the managed clients that do not connect, Symantec Endpoint Protection Manager deletes clients from the database after 30 days by default. You can change the period of time after which Symantec Endpoint Protection Manager deletes the client from the database. By deleting a client, you also save space in the database.</p> <p> <a href="#">Uninstalling the Symantec Endpoint Protection client for Windows</a>  <a href="#">Uninstalling the Symantec Endpoint Protection client for Mac</a>  <a href="#">Uninstalling the Symantec Endpoint Protection client for Linux</a>  <a href="#">Purging obsolete clients from the database to make more licenses available</a> </p>

## Viewing the protection status of client computers

You can view information about the real-time operational and protection status of the clients and the computers in your network.

You can view:

- A list of managed client computers that do not have the client installed.  
You can view the computer name, the domain name, and the name of the user who is logged on.
- Which protections are enabled and disabled.
- Which client computers have the latest policies and definitions.
- The group's policy serial number and the client's version number.
- The information about the client computer's network components, such as the MAC address of the network card that the computer uses.
- The system information about the client computer, such as the amount of available disk space and the operating system version number.

After you know the status of a particular client, you can resolve any security issues on the client computers. You can resolve many issues by running commands on groups. For example, you can update content, or enable Auto-Protect.

### NOTE

If you manage any clients that run an earlier version of Symantec Endpoint Protection, some newer protection technologies may be listed as **not reporting**. This behavior is expected. It does not mean that you need to take action on these clients.

[Checking whether the client is connected to the management server and is protected](#)

[Running commands on client computers from the console](#)

[Searching for the clients that do not have the client software installed](#)

- In the console, click **Clients**.
- On the **Clients** page, under **Clients**, locate the group that contains the clients that you want information about.
- On the **Clients** tab, click the **View** drop-down list. Then, select a category.

You can go directly to a particular page by typing the page number in the text box at the bottom right-hand corner.

---

## Enabling protection on the client computer

You should keep all types of protection enabled on your computer at all times, especially Auto-Protect.

On the client, when any of the protections are disabled:

- The status bar is red at the top of the **Status** page.
- The client's icon appears with a universal no sign, a red circle with a diagonal slash. The client icon appears as a full shield in the taskbar in the lower-right corner of your Windows desktop. In some configurations, the icon does not appear.

[Symantec Endpoint Protection client status icons](#)

On a managed client, your administrator can enable or disable a protection technology at any time. If you disable a protection, your administrator may later enable the protection again. Your administrator might also lock a protection so that you cannot disable it.

### To enable protection technologies from the Status page:

1. On the client, at the top of the **Status** page, click **Fix** or **Fix All**.

### To enable protection technologies from the taskbar:

1. On the Windows desktop, in the notification area, right-click the client icon, and then click **Enable Symantec Endpoint Protection**.

### To enable protection technologies from within the client:

1. In the client, on the **Status** page, beside the protection type, click **Options > Enable the <protection type>**.

### To enable the firewall:

1. On the client, at the top of the **Status** page, next to **Network and Host Exploit Mitigation**, click **Options > Change Settings**.
2. On the **Firewall** tab, check **Enable Firewall**.
3. Click **OK**.

## Searching for the clients that do not have the client software installed

You can search for clients in a group based on the following criteria:

- Client software is installed.
- Clients run on Windows, Mac, or Linux computers
- Windows clients are in computer mode or user mode.
- Clients are non-persistent and offline in Virtual desktop infrastructures.

[Viewing the protection status of client computers](#)

---

### Checking whether the client is connected to the management server and is protected

1. In the console, click **Clients**.
2. In the **Clients** pane, choose the group you want to search on.
3. On the **Clients** tab, under **Tasks**, click **Set display filter**.
4. In the **Set Display Filter** dialog box, check **New users or computers that have been created but that don't yet have the client software installed**.
5. Click **OK**.

## Searching for information about client computers

You can search for information about the clients, client computers, and users to make informed decisions about the security of your network.

For example, you can find which computers in the Sales group run the latest operating system. You can find out which client computers in the Finance group need the latest virus definitions installed.

### NOTE

To search for most of the information about the users, you must collect user information either during the client software installation or later. This user information is also displayed on the General tab and the User Info tab in the client's Edit Properties dialog box.

### Collecting user information

1. In the console, click **Clients**.
2. Under **Tasks**, click **Search clients**.
3. In the **Search clients** dialog box, in the **Find** drop-down list, click either **Computers** or **Users**.
4. Click **Browse** to select a group other than the default group. Click to select the group, and then click **OK**.
5. Under **Search Criteria**, click in the **Search Field** to see the drop-down list, and then select the criteria by which you want to search.

To find embedded clients, you can search for the type of write filters in use. Click **Enhanced Write Filter**, **File Based Write Filter**, or **Unified Write Filter** to search for whether they are installed, enabled, or both. You can also search for the reduced-size client. Click **Install Type** to search for a value of **Reduced Size**.

6. Click the **Comparison Operator** drop-down list, and then select a comparison operator.

You can use standard Boolean operators in your search criteria. Click **Help** for more information on the options.

7. In the **Value** cell, type the search string.
8. Click **Search**.

You can export the results into a text file.

9. Click **Close**.

You can export the data that is contained in the query into a text file.

### Viewing the protection status of client computers

## What are the commands that you can run on client computers?

You can run commands remotely on individual clients or an entire group from the console.

To see the results of any of the commands, click **Monitors** page > **Logs** > **Command Status**. You can also run some of the commands from the **of type** drop-down list.

System administrators and domain administrators can run these commands automatically. For limited administrators, you enable or disable access for each command individually.

[Adding an administrator account and setting access rights](#)

[Running commands on client computers from the console](#)

**Table 62: Commands that you can run on client computers**

Commands	Description
<b>Analyze</b> (Removed in 14.3)	In earlier releases, the <b>Analyze</b> command showed the progress of all requests that you submitted for analysis from the cloud console to the Content Analysis System (CAS).
<b>Cancel Evidence of Compromise Scan</b>	Starts or cancels a scan that you use on third-party remote monitoring and management.
<b>Scan</b>	<p>Runs an on-demand scan on the client computers.</p> <p>If you run a scan command, and select a <b>Custom</b> scan, the scan uses the command scan settings that you configured on the <b>Administrator-defined Scans</b> page. The command uses the settings that are in the Virus and Spyware Protection policy that is applied to the selected client computers.</p> <p><a href="#">Running on-demand scans on client computers</a></p> <p><b>Note:</b> You can run only a custom scan on Mac client computers.</p>
<b>Update Content</b>	<p>Updates content on clients by initiating a LiveUpdate session on the client computers. The clients receive the latest content from Symantec LiveUpdate.</p> <p><a href="#">Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager</a></p>
<b>Update Content and Scan</b>	Updates content by initiating a LiveUpdate session and runs an on-demand scan on client computers.
<b>Start Power Eraser Analysis</b>	<p>Runs a Power Eraser analysis on the selected computers. You should typically run Power Eraser only on a single computer or a small number of computers. You should only run Power Eraser when computers exhibit instability or have persistent problems. Unlike other scans, Power Eraser does not automatically remediate any potential threats. You must review the detections in the logs and specify which risks you want to remove or leave alone.</p> <p><b>Note:</b> Mac and Linux client computers do not process this command.</p> <p><a href="#">Starting Power Eraser analysis from Symantec Endpoint Protection Manager</a></p>
<b>Restart Client Computers</b>	<p>Restarts the client computers.</p> <p>If users are logged on to the client, they are warned based on the restart options that the administrator has configured for that client. You can configure client restart options on the <b>General Settings</b> page.</p> <p><b>Note:</b> Restart options apply only to Windows client computers. Mac client computers always perform a hard restart. Linux client computers ignore this command.</p> <p><a href="#">Restarting the client computers from Symantec Endpoint Protection Manager</a></p> <p><b>Note:</b> You can ensure that a Windows client does not restart. You can add a registry key on the client that keeps it from restarting even if an administrator issues a restart command.</p> <p><b>Note:</b> <a href="#">Ensuring that a client does not restart</a></p>
<b>Enable Auto-Protect</b>	<p>Enables Auto-Protect for the file system on the client computers.</p> <p>By default, Auto-Protect for the file system is enabled. Symantec recommends that you always keep Auto-Protect enabled. You can lock the setting so that users on client computers cannot disable Auto-Protect.</p> <p><a href="#">Customizing Auto-Protect for Windows clients</a></p> <p><a href="#">Customizing Auto-Protect for Mac clients</a></p> <p>If Auto-Protect for email is disabled, you enable it in the Virus and Spyware Protection policy.</p>



Commands	Description
<b>Enable Network Threat Protection and Disable Network Threat Protection</b>	Enables or disables the firewall and enables intrusion prevention on the client computers. <b>Note:</b> Linux client computers do not process this command. <a href="#">Managing firewall protection</a>
<b>Enable Download Insight and Disable Download Insight</b>	Enables or disables Download Insight on the client computers. <b>Note:</b> Mac and Linux client computers do not process this command. <a href="#">Managing Download Insight detections</a>
<b>Delete From Quarantine</b>	Deletes all files from Quarantine. This command only appears on the <b>Risk</b> log > <b>Action</b> drop-down list. <a href="#">How to delete Quarantined items from the Symantec Endpoint Protection Manager</a>
<b>Collect file fingerprint list</b>	Generates a non-editable file fingerprint list from the selected clients. The collected fingerprint list appears on the <b>Policies</b> tab under <b>Policy Components &gt; File Fingerprint Lists</b> . Typically, you run this command on a single computer or small group of computers. If you select multiple computers, the command collects a separate list for each computer. <b>Note:</b> Mac and Linux client computers do not process this command.
<b>Place Client(s) in Quarantine and Remove Client(s) From Quarantine</b>	Lets you add clients to or remove clients from Quarantine. These commands are only available when you enable Deception.
<b>Send Logs to Symantec</b>	Collects the information about a Windows client computer that either crashes or behaves unexpectedly. You run this command after you have called Technical Support, who asks for the event ID of the client that crashed. To find the event ID, click <b>Monitors &gt; Command Status &gt; Details</b> . You should not use this command if your company has a restrictive data protection policy. <a href="#">Enabling the management server to send information to Symantec about a client that crashed</a>

## [Symantec Endpoint Protection features based on platform](#)

## Running commands on client computers from the console

You can manually run commands on the client computer at any time, such as starting or canceling a scan. On managed clients, the commands that you run from the management server override the commands that the user runs. The order in which commands are processed on the client computer differs from command to command. Regardless of where the command is initiated, the commands are processed in the same way.

### [What are the commands that you can run on client computers?](#)

You run these commands from the following locations:

- The **Clients** page.
- The **Computer Status** log. You can run the **Cancel All scans** and **Start Power Eraser Analysis** commands from the **Computer Status** log only.
- The **Risk** Log. You can run the **Delete from Quarantine** command from the **Risk** log only.  
[How to delete Quarantined items from the Symantec Endpoint Protection Manager](#)

If you start a scan, you can also cancel it immediately.

1. To run commands on the client computer from the **Clients** page, in the console, click **Clients**.
2. Do one of the following actions for groups or computers:
  - In the left pane, right-click the group, and then click **Run a command on the group > command**
  - Click the **Clients** tab, right-click the computers, and then click **Run command on computers > command**

- 
3. In the message that appears, click **Yes**.
  4. To run a command from the Computer Status log, click **Monitors > Logs > the Computer Status** log type, and then click **View Log**.
  5. Select a command from the **Command** list box, select the computers, and then click **Start**.

**NOTE**

You can cancel an in-progress scheduled scan or a scan that you started by clicking **Cancel All Scans** from the command list.

6. Click **Monitors**.
7. On the **Command Status** tab, select a command in the list, and then click **Details**.

**NOTE**

You can also cancel a scan in progress by clicking the **Cancel Scan** icon in the **Command** column of the scan command.

## Ensuring that a client does not restart

You can use the following procedure to ensure that any Symantec Endpoint Protection client computer does not restart. For example, you may want to set this value on the servers that run the Symantec Endpoint Protection client. Setting this registry key ensures that the server does not restart if an administrator issues a Restart computer command on its group from the console.

To ensure that a client does not restart

1. On the client computer, open the registry editor.
2. Navigate to HKEY\_LOCAL\_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC.
3. Add the following line to the registry:

```
DisableRebootCommand    REG_DWORD    1
```

## Switching a Windows client between user mode and computer mode

You add Windows clients to be in either user mode or computer mode, based on how you want to apply policies to the clients in groups. After a user or a computer is added to a group, it assumes the policies that were assigned to the group.

When you add a client, it defaults to computer mode, which takes precedence over user mode. Symantec recommends that you use computer mode. Linux clients and Mac clients are only installed in computer mode.

Mode	Description
Computer mode	<p>The client computer gets the policies from the group of which the computer is a member. The client protects the computer with the same policies, regardless of which user is logged on to the computer. The policy follows the group that the computer is in. Computer mode is the default setting. Many organizations configure a majority of clients in computer mode. Based on your network environment, you might want to configure a few clients with special requirements as users.</p> <p>You cannot switch from user mode to computer mode if the computer name is already in another group. Switching to computer mode deletes the user name of the client from the group and adds the computer name of the client into the group.</p> <p>Clients that you add in computer mode can be enabled as unmanaged detectors, and used to detect unauthorized devices.</p> <p><a href="#">Configuring a client to detect unmanaged devices</a></p>
User mode	<p>The client computer gets the policies from the group of which the user is a member. The policies change, depending on which user is logged on to the client. The policy follows the user.</p> <p>If you import your existing group structure into Symantec Endpoint Protection Manager from Microsoft Active Directory or LDAP directory servers to organize clients by user, use user mode.</p> <p>You cannot switch from computer mode to user mode if the user's logon name and the computer name are already contained in any group. Switching to user mode deletes the computer name of the client from the group. It then adds the user name of the client into the group.</p> <p><a href="#">Importing existing groups and computers from an Active Directory or an LDAP server</a></p>

When you deploy a client installation package, you specify which group the client goes in. You can later specify the client to be in user mode or computer mode. If the client later gets deleted or disconnected and then gets added again and reconnected, the client returns to the original group. However, you can configure the client to stay with the group it was last moved to in user mode or computer mode. For example, a new user might log on to a client that is configured in user mode. The client then stays in the group that the previous user was in.

You configure these settings by clicking **Clients > Policies**, and then **Communications Settings**.

#### [Communications Settings for <group\\_name>](#)

To switch a Windows client between user mode and computer mode

1. In the console, click **Clients**.
2. On the **Clients** page, under **Clients**, select the group that contains the user or computer.
3. On the **Clients** tab, right-click the computer or the user name in the table, and then select either **Switch to Computer Mode** or **Switch to User Mode**.

This mode is a toggle setting so one or the other always displays. The information in the table changes to reflect the new setting.

## Configuring a client to detect unmanaged devices

Unauthorized devices can connect to the network in many ways, such as physical access in a conference room or rogue wireless access points. To enforce policies on every endpoint, you must be able to quickly detect the presence of new devices in your network. You must determine whether the devices are secure. You can enable any client as an unmanaged detector to detect the unknown devices. Unknown devices are unmanaged devices that do not run Symantec Endpoint Protection client software. If the unmanaged device is a computer, you can install the Symantec Endpoint Protection client software on it.

When a device starts up, its operating system sends the following traffic to the network to let other computers know of the device's presence:

- 
- Address Resolution Protocol (ARP) traffic (ICMPv4)
  - Neighbor Discovery Protocol (NDP) traffic (ICMPv6).
- ICMPv6 is supported as of version 14.2.

A client that is enabled as an unmanaged detector collects and sends this packet information to the management server. The management server searches the packet for the device's MAC address and the IP address. The server compares these addresses to the list of existing MAC and IP addresses in the server's database. If the server cannot find an address match, the server records the device as new. You can then decide whether the device is secure. Because the client only transmits information, it does not use additional resources.

You can configure the unmanaged detector to ignore certain devices, such as printers. You can also set up email notifications to notify you when the unmanaged detector detects an unknown device.

To configure the client as an unmanaged detector, you must do the following actions:

- Enable Network Threat Protection.  
[Running commands on client computers from the console](#)
- Switch the client to computer mode.  
[Switching a Windows client between user mode and computer mode](#)
- Install the client on a computer that runs all the time.

As of 14.3 RU1, enabling the Linux client as an unmanaged detector is deprecated.

#### To configure an unmanaged detector:

1. In the console, click **Clients**.
2. Under **Clients**, select the group that contains the client that you want to enable as an unmanaged detector.
3. On the **Clients** tab, right-click the client that you want to enable as an unmanaged detector, and then click **Enable as Unmanaged Detector**.
4. To specify one or more devices to exclude from detection by the unmanaged detector, click **Configure Unmanaged Detector**.
5. In the **Unmanaged Detector Exceptions for client name** dialog box, click **Add**.
6. In the **Add Unmanaged Detector Exception** dialog box, click one of the following options:
  - **Exclude detection of an IP address range**, and then enter the IP address range for several devices.
  - **Exclude detection of a MAC address**, and then enter the device's MAC address.
7. Click **OK** > **OK**.
8. To display the list of unauthorized devices that the client detects, in the console, click **Home**.
9. On the **Home** page, in the **Security Status** section, click **More Details**.
10. In the **Security Status Details** dialog box, scroll to the **Unknown Device Failures** table.
11. Close the dialog box.

#### To see if unmanaged clients are being detected:

1. Go to the **Home** page and click **View Details** in the **Security Status** area.
2. When the **Security Status Details** window appears, click **Unknown Device Failures**.  
**Total Detected Unknown Devices** shows how many devices are unmanaged. This includes access points, routers, switches and other devices in addition to computers.
3. To filter extraneous devices, go to the **Clients** page and right-click the unmanaged detector.
4. Click **Configure Unmanaged Detector** and add the IP or Mac addresses of the devices to be filtered.

## Password-protecting the Symantec Endpoint Protection client

You can increase corporate security by requiring password protection on the client computer whenever users perform certain tasks.

**You can require the users to type a password when users try to do one of the following actions:**

- 
- Open the client's user interface.
  - Stop the client service.
  - Uninstall the client.

#### NOTE

This option works on the Windows client only.

- Import and export the client communication settings.

### Preventing and allowing users to change the client's user interface

To password-protect the client

1. In the console, click **Clients**.
2. Under **Clients**, select the group for which you want to set up password protection.
3. On the **Policies** tab, under **Location-independent Policies and Settings**, click **Password**.

Earlier versions of Symantec Endpoint Protection may have some options that are worded differently, but you can still password-protect the client from the **Policies** tab.

4. In the **Client Password Settings** window, check any or all of the check boxes.

If the boxes are grayed out, this group inherits policies from a parent group. Before you can proceed, you must either edit the policy in the parent group or disable inheritance for this group.

#### Disabling a group's inheritance

5. In the **Password** and **Confirm password** text boxes, type the same password.

You can create a password that is between 6 to 256 characters in length.

If you see a message that the password strength is not acceptable, consider increasing the strength of your password. However, you may still be able to save the password.

Check **Apply password settings to non-inherited sub groups** to modify the password protection settings for any child group that does not inherit its settings from a parent. This setting appears for a parent group only.

6. Click **OK**.

## Preventing and allowing users to change the client's user interface

### What can users change on the client user interface?

You as the administrator set the user control level to determine whether the user can make changes to the client. For example, you can prevent the user from opening the client user interface or the notification area icon. The user interface features that you manage for the users are called managed settings. The user does not have access to all of the client features, such as password protection.

### Password-protecting the Symantec Endpoint Protection client

#### How do I configure user interface settings?

**You can configure user interface settings on the client if you do either of the following tasks:**

- Set the client's user control level to server control.
- Set the client's user control level to mixed control and set the parent feature on the **Client/Server Control Settings** tab to **Server**.

For example, you can set the **Show/Hide notification area icon** option to **Client**. The notification area icon appears on the client and the user can choose to show or hide the icon. If you set the **Show/Hide notification area icon** option to **Server**, you can choose whether to display the notification area icon on the client.

---

## NOTE

Most of these settings apply to the Windows client only. You can configure a few options on the Mac client in server control only.

1. To configure user interface settings in mixed control, click **Clients > Policies** tab.

[Preventing users from disabling protection on client computers](#)

2. In the **Client User Interface Control Settings for location name** dialog box, next to **Mixed control**, click **Customize**.
3. In the **Client User Interface Mixed Control Settings** dialog box, on the **Client/Server Control Settings** tab, do one of the following actions:
  - Lock an option so that you can configure it only from the server. For the option you want to lock, click **Server**. Any Virus and Spyware Protection settings that you set to Server here override the settings on the client.
  - Unlock an option so that the user can configure it on the client. For the option you want, click **Client**. Client is selected by default for all settings except the virus and spyware settings.
4. For some of the options that you set to **Server**, click the **Client User Interface Settings** tab to configure them:

For information on where in the console you configure the remaining options that you set to **Server**, click **Help**. For example, to enable firewall settings, configure them in the Firewall policy.

[Enabling communications for network services instead of adding a rule](#)

[Enabling network intrusion prevention or browser intrusion prevention](#)

5. On the **Client User Interface Settings** tab, check the option's check box so that the option is available on the client.
6. Click **OK**.
7. Click **OK**.
8. To configure user interface settings in server control, change the user control level to server control.

[Preventing users from disabling protection on client computers](#)

9. In the **Client User Interface Settings** dialog box, check the options that you want to appear on the client.
10. Click **OK**.
11. Click **OK**.

[Configuring firewall settings for mixed control](#)

## Collecting user information

You can prompt users on the client computers to type information about themselves during the client software installation process or during policy updates. You can collect information such as the employee's mobile phone number, job title, and email address. After you collect this information, you must maintain and update it manually.

## NOTE

After you enable the message to appear on the client computer for the first time, and the user responds with the requested information, the message does not appear again. Even if you edit any of the fields or disable and enable the message again, the client does not display a new message. However, the user can edit the information at any time, and the management server retrieves that information.

[Managing client installation packages](#)

To collect user information

- 
1. In the console, click **Admin**, and then click **Install Packages**.
  2. In the **Install Packages** pane, click **Client Install Packages**.
  3. Under **Tasks**, click **Set User Information Collection**.
  4. In the **Set User Information Collection** dialog box, check **Collect User Information**.
  5. In the **Pop-up Message** text box, type the message that you want users to read when they are prompted for information.
  6. If you want the user to have the ability to postpone user information collection, check **Enable Remind Me Later**, and then set a time in minutes.
  7. Under **Select the fields that will be displayed for the user to provide input**, choose the type of information to collect, and then click **Add**.

You can select one or more fields simultaneously by pressing the Shift key or the Control key.

8. In the Optional column, check the check box next to any fields that you want to define as optional for the user to complete.
9. Click **OK**.

## Checking on your Mac client using AppleScript scripts

(For 14.3 RU2 and later)

AppleScript integration with Symantec Endpoint Protection client for Mac lets you create and run AppleScript scripts to query or control your Mac client.

Predefined scripts for querying the Mac client are not available. You will have the flexibility to create the scripts according to your requirements.

You can create and run the scripts in the Script Editor or you can run them from the command line. Using the Mac features, you can also schedule the scripts to run automatically at a specified time.

### To create and run an AppleScript script in the Script Editor

1. On your Mac device, open the Script Editor, and create a script that you want to run on your Mac device.  
You can use the script examples given below.
2. To test the script, click **Run** on the toolbar.
3. Save the script in a format that best meets your needs.

### To run an AppleScript script from the command line

1. On your Mac device, open the Terminal window.
2. Run the script that you want.

**Table 63: Examples of AppleScript scripts for Mac client**

Action	Script Examples
Get last scan time	Script to run in the Script Editor: tell application "Symantec Endpoint Protection" get last scan time end tell Script to run from the command line: osascript -e 'tell app "Symantec Endpoint Protection" to get last scan time'
Get product version	Script to run in the Script Editor: tell application "Symantec Endpoint Protection" get version end tell Script to run from the command line: osascript -e 'tell app "Symantec Endpoint Protection" to get version'
Get content versions	Script to run in the Script Editor: tell application "Symantec Endpoint Protection" get definition information end tell Script to run from the command line: osascript -e 'tell app "Symantec Endpoint Protection" to get definition information'
Run LiveUpdate	Script to run in the Script Editor: tell application "Symantec Endpoint Protection" activate tell main window to run LiveUpdate end tell Script to run from the command line: osascript -e 'tell app "Symantec Endpoint Protection" -e 'activate' -e 'tell main window to run LiveUpdate' -e 'end tell'
Run QuickScan	Script to run in the Script Editor: tell application "Symantec Endpoint Protection" activate tell main window to quick scan end tell Script to run from the command line: osascript -e 'tell app "Symantec Endpoint Protection" -e 'activate' -e 'tell main window to quick scan' -e 'end tell'

## Managing your Linux client using the command line tool (sav)

(For 14.3 RU2 and later)

The Linux client command line tool lets you control and check on your Linux client.

### To manage your Linux client using the command line tool

1. On a Linux client computer, navigate to the following location:  
/opt/Symantec/sdcssagent/AMD/tools
2. Run the sav command as follows:  
./sav [options] command



**Table 64: Options for sav**

Option	Description	Applies to
-q	Quiet	As of 14.3 RU2
-h	Displays available options and commands for sav.	As of 14.3 RU2

**Table 65: Commands for sav**

Option	Description	Applies to
autoprotect -e	Enables Auto-Protect. To check the Auto-Protect status, run the following command: [root@localhost tools]# cat /proc/sisap/status   grep -i MODE The reply can be one of the following: <ul style="list-style-type: none"> <li>mode=ENA (if enabled)</li> <li>mode=DIS (if disabled)</li> </ul>	As of 14.3 RU2
autoprotect -d	Disables Auto-Protect.	As of 14.3 RU2
info -d	Shows the version and date of the current virus and security risk definitions in use on the device.	As of 14.3 RU3
info -e	Shows the version of the scan engine in use on the device.	As of 14.3 RU3
info -p	Shows the Symantec Agent version in use on the device.	As of 14.3 RU3
info -a	Shows the status of Auto-Protect on the device.	As of 14.3 RU3
liveupdate -u	Runs LiveUpdate immediately.	As of 14.3 RU3
manage -i <file>	Imports the <i>sylink.xml</i> file to the specified location.	As of 14.3 RU2
manualscan -s <file list>	Starts a manual scan. <file list> specifies the file and directory list to scan. To specify this list, type a list of files and directories separated by line feeds and ending with an end of file signal, such as CTRL-D. If a directory is specified, all subdirectories are also scanned. Wildcard characters are supported. By default, the maximum number of items that can be added to a manual scan that is started from the command line interface is 100. You can use <b>symcfg</b> to change the DWORD value of VirusProtect6MaxInput to increase this limit. To remove the limit entirely, set the value of VirusProtect6MaxInput to 0. If you specify a hyphen (-) instead of a list of files and directories, then the list of path names is read from the standard input. You can use commands that produce a list of files or path names separated by line feeds. Submitting a very long list of items to this command can negatively affect performance. Symantec recommends that you limit lists to a maximum of a few thousand items.	As of 14.3 RU3
manualscan -t	Stops a manual scan that is in progress.	As of 14.3 RU3

## Troubleshooting the Symantec Linux Agent

## Managing remote clients

Your network may include some clients that connect to the network from different locations. You may need to manage these clients differently from the clients that connect only from within the network. You may need to manage some clients that always connect remotely over a VPN, or clients that connect from multiple locations because employees travel. You may also need to manage security for some computers that are outside your administrative control. For example, you may

---

allow customers, contractors, vendors, or business partners to have limited access to your network. Some employees may connect to your network using their own personal computers, and you may need to manage these clients differently.

In all these cases, you must deal with greater security risk. Connections may be less secure, or the client computers may be less secure, and you may have less control over some clients. To minimize these risks to your overall network security, you should assess the different kinds of remote access that clients have to your network. You can then apply more stringent security policies based on your assessment.

To manage the clients that connect to your network differently because of the security risks that they pose, you can work with Symantec Endpoint Protection's location awareness.

You apply different policies to clients that pose a greater risk to your network based on their location. A location in Symantec Endpoint Protection is defined as the type of connection that a client computer uses to connect to your network. A location can also include information about whether the connection is located inside or outside your corporate network.

You define locations for a group of clients. You then assign different policies to each location. Some security settings can be assigned to the entire group regardless of location. Some settings are different depending on location.

**Table 66: Managing remote clients**

Task	Description
Set up groups based on assessment of security risk	<a href="#">Managing groups of clients</a>
Set up locations for groups of remote clients	<a href="#">Managing locations for remote clients</a>
Configure communication settings for locations	<a href="#">Configuring communication settings for a location</a>
Strengthen your security policies	<a href="#">About strengthening your security policies for remote clients</a>
Turn on client notifications	<a href="#">About turning on notifications for remote clients</a>
Customize client log management settings	Customize the log settings for remote clients, especially if clients are offline for several days. To reduce bandwidth and the load on your management servers, make the following changes: <ul style="list-style-type: none"><li>• Set clients to not upload their logs to the management server.</li><li>• Set clients to upload only the client security logs.</li><li>• Set filter log events to upload only specified events. Suggested events to upload include definition updates, or side effect repair failures.</li><li>• Make the log retention time longer. Longer retention times let you review more virus and spyware event data.</li></ul>
Monitor remote clients	<a href="#">About monitoring remote clients from the management server</a> <a href="#">Monitoring roaming Symantec Endpoint Protection clients from the cloud console</a>

## Managing locations for remote clients

You add locations after you set up the groups that you need to manage. Each group can have different locations if your security strategy requires it. In the Symantec Endpoint Protection Manager console, you set up the conditions that trigger automatic policy switching based on location. Location awareness automatically applies the security policy that you specify to a client, based on the location conditions that the client meets.

Location conditions can be based on a number of different criteria. These criteria include IP addresses, type of network connection, whether the client computer can connect to the management server, and more. You can allow or block client connections based on the criteria that you specify.

---

A location applies to the group you created it for and to any subgroups that inherit from the group. A best practice is to create the locations that any client can use at the My Company group level. Then, create locations for a particular group at the subgroup level.

It is simpler to manage your security policies and settings if you create fewer groups and locations. The complexity of your network and its security requirements, however, may require more groups and locations. The number of different security settings, log-related settings, communications settings, and policies that you need determines how many groups and locations you create.

Some of the configuration options that you may want to customize for your remote clients are location-independent. These options are either inherited from the parent group or set independently. If you create a single group to contain all remote clients, then the location-independent settings are the same for the clients in the group.

**The following settings are location-independent:**

- Custom intrusion prevention signatures
- System Lockdown settings
- Network application monitoring settings
- LiveUpdate content policy settings
- Client log settings
- Client-server communications settings
- General security-related settings, including location awareness and Tamper Protection

To customize any of these location-independent settings, such as how client logs are handled, you need to create separate groups.

Some settings are specific to locations.

**As a best practice, you should not allow users to turn off the following protections:**

- Auto-Protect
- SONAR
- Tamper Protection
- The firewall rules that you have created

**Table 67: Location awareness tasks that you can perform**

Tasks	Description
Plan locations	You should consider the different types of security policies that you need in your environment to determine the locations that you should use. You can then determine the criteria to use to define each location. It is a best practice to plan groups and locations at the same time. <a href="#">Managing groups of clients</a> You may find the following examples helpful: <a href="#">Setting up Scenario One location awareness conditions</a> <a href="#">Setting up Scenario Two location awareness conditions</a>
Enable location awareness	To control the policies that are assigned to clients contingent on the location from which the clients connect, you can enable location awareness. <a href="#">Enabling location awareness for a client</a>
Add locations	You can add locations to groups. <a href="#">Adding a location to a group</a>

Tasks	Description
Assign default locations	<p>All groups must have a default location. When you install the console, there is only one location, called Default. When you create a new group, its default location is always Default. You can change the default location later after you add other locations.</p> <p>The default location is used if one of the following cases occurs:</p> <ul style="list-style-type: none"> <li>• One of the multiple locations meets location criteria and the last location does not meet location criteria.</li> <li>• You use location awareness and no locations meet the criteria.</li> <li>• The location is renamed or changed in the policy. The client reverts to the default location when it receives the new policy.</li> </ul> <p><a href="#">Changing a default location</a></p>
Configure communications settings for locations	<p>You can also configure the communication settings between a management server and the client on a location basis.</p> <p><a href="#">Configuring communication settings for a location</a></p>

See the article [Best Practices for Symantec Endpoint Protection Location Awareness](#).

### [Managing remote clients](#)

## Enabling location awareness for a client

To make the policies that are assigned to clients contingent on the client's connection location, you can enable location awareness for the client.

If you check **Remember the last location**, then when a client connects to the network, it is assigned the policy from the last-used location. If location awareness is enabled, then the client automatically switches to the appropriate policy after a few seconds. The policy that is associated with a specific location determines a client's network connection. If location awareness is disabled, the client can manually switch between any of the locations even when it is under server control. If a quarantine location is enabled, the client may switch to the quarantine policy after a few seconds.

If you uncheck **Remember the last location**, then when a client connects to the network, it is assigned the policy from the default location. The client cannot connect to the last-used location. If location awareness is enabled, then the client automatically switches to the appropriate policy after a few seconds. The policy that is associated with a specific location determines a client's network connection. If location awareness is disabled, the user can manually switch between any of the locations even when the client is under server control. If a quarantine location is enabled, the client may switch to the Quarantine Policy after a few seconds.

1. In the console, click **Clients**.
2. On the **Clients** page, under **Clients**, select the group for which you want to implement automatic switching of locations.
3. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.
4. Under **Location-independent Policies and Settings**, click **General Settings**.
5. In the **General Settings** dialog box, on the **General Settings** tab, under **Location Settings**, check **Remember the last location**.

By default, this option is enabled. The client is initially assigned to the policy that is associated with the location from which the client last connected to the network.

6. Check **Enable Location Awareness**.

By default, location awareness is enabled. The client is automatically assigned to the policy that is associated with the location from which the user tries to connect to the network.

- 
7. Click **OK**.

#### [Adding a location to a group](#)

## Adding a location to a group

When you add a location to a group, you specify the conditions that trigger the clients in the group to switch to the location. Location awareness is effective only if you also apply appropriate policies and settings to each location.

To add a location to a group

1. In the console, click **Clients**.
2. In the **Clients** page, under **Clients**, select the group for which you want to add one or more locations.
3. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.  
You can add locations only to groups that do not inherit policies from a parent group.  
You can also click **Add Location** to run the **Add Location** wizard.
4. In the **Client** page, under **Tasks**, click **Manage Locations**.
5. In the **Manage Locations** dialog box, under **Locations**, click **Add**.
6. In the **Add Location** dialog box, type the name and description of the new location, and then click **OK**.
7. To the right of the **Switch to this location when** box, click **Add**.
8. In the **Type** list, select a condition, and then select the appropriate definition for the condition.  
A client computer switches to the location if the computer meets the specified criteria.
9. Click **OK**.
10. To add more conditions, click **Add**, and then select either **Criteria with AND relationship** or **Criteria with OR relationship**.
11. Click **OK**.

#### [About strengthening your security policies for remote clients](#)

## Changing a default location

When the Symantec Endpoint Protection Manager is initially installed, only one location, called Default, exists. At that time, every group's default location is Default. Every group must have a default location. When you create a new group, the Symantec Endpoint Protection Manager console automatically makes its default location Default.

You can specify another location to be the default location for a group after you add other locations. You may prefer to designate a location like Home or Road as the default location.

### **A group's default location is used if one of the following cases occurs:**

- One of the multiple locations meets location criteria and the last location does not meet location criteria.
- You use location awareness and no locations meet the criteria.
- The location is renamed or changed in the policy. The client reverts to the default location when it receives the new policy.

To change a default location

- 
1. In the console, click **Clients**.
  2. On the **Clients** page, under **Clients**, click the group to which you want to assign a different default location.
  3. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.
  4. Under **Tasks**, click **Manage Locations**.
  5. In the **Manage Locations** dialog box, under **Locations**, select the location that you want to be the default location.
  6. Under **Description**, check **Set this location as the default location in case of conflict**.  
The Default location is always the default location until you assign another one to the group.
  7. Click **OK**.

#### [Managing locations for remote clients](#)

### Setting up Scenario One location awareness conditions

If you have remote clients, in the simplest case, it is a common practice to use the My Company group and three locations. This is Scenario One.

**To manage the security of the clients in this scenario, you can create the following locations under the My Company group to use:**

- Office clients that log on in the office.
- The remote clients that log on to the corporate network remotely over a VPN.
- The remote clients that log on to the Internet remotely, but not over a VPN.

Because the remote location with no VPN connection is the least secure, it has the most secure policies. It is a best practice to always make this location the default location.

#### **NOTE**

If you turn off My Company group inheritance and then you add groups, the added groups do not inherit the locations that you set up for the My Company group.

---

The following suggestions represent the best practices for Scenario One.

1. To set up the office location for the clients located in the office, on the **Clients** page, select the group for which you want to add a location.
2. On the **Policies** tab, under **Tasks**, click **Add Location**.
3. In the **Add Location Wizard**, click **Next**.
4. Type a name for the location and optionally, add a description of it, and then click **Next**.
5. In the list box, click **Client can connect to management server** from the list, and then click **Next**.
6. Click **Finish**, and then click **OK**.
7. Under **Tasks**, click **Manage Locations**, and then select the location you created.
8. Click **Add**, and then click **Criteria with AND relationship**.
9. In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.
10. Click **If the client computer does not use the network connection type specified below**.
11. In the bottom list box, select the name of the VPN client that your organization uses, and then click **OK**.
12. Click **OK** to exit the **Manage Locations** dialog box.
13. To set up the remote location for the clients logging in over a VPN, on the **Clients** page, select the group for which you want to add a location.
14. On the **Policies** tab, under **Tasks**, click **Add Location**.
15. In the **Add Location Wizard**, click **Next**.
16. Type a name for the location and optionally, add a description of it, and then click **Next**.
17. In the list box, click **Network connection type**.
18. In the **Connection Type** list box, select the name of the VPN client that your organization uses, and then click **Next**.
19. Click **Finish**.
20. Click **OK**.
21. To set up the remote location for the clients not logging on over a VPN, on the **Clients** page, select the group for which you want to add a location.
22. On the **Policies** tab, under **Tasks**, click **Add Location**.
23. In the **Add Location Wizard**, click **Next**.
24. Type a name for the location, optionally add a description of it, and then click **Next**.
25. In the list box, leave **No specific condition**, and then click **Next**.

By using these settings, this location's policies, which should be the strictest and most secure, are used as the default location policies.
26. Click **Finish**, and then click **OK**.

[Setting up Scenario Two location awareness conditions](#)

[Managing remote clients](#)

---

## Setting up Scenario Two location awareness conditions

In Scenario Two, you use the same two remote locations as specified in Scenario One and two office locations, for a total of four locations.

**You would add the following office locations:**

- Clients in the office that log on over an Ethernet connection.
- Clients in the office that log on over a wireless connection.

It simplifies management to leave all clients under the default server control mode. If you want granular control over what your users can and cannot do, an experienced administrator can use mixed control. A mixed control setting gives the end user some control over security settings, but you can override their changes, if necessary. Client control allows users a wider latitude in what they can do and so constitutes a greater risk to network security.

**Symantec suggests that you use client control only in the following situations:**

- If your users are knowledgeable about computer security.
- If you have a compelling reason to use it.

### NOTE

You may have some clients that use Ethernet connections in the office while other clients in the office use wireless connections. For this reason, you set the last condition in the procedure for wireless clients in the office. This condition lets you create an Ethernet location Firewall policy rule to block all wireless traffic when both kinds of connections are used simultaneously.

**To set up the office location for the clients that are logged on over Ethernet**

1. On the **Clients** page, select the group for which you want to add a location.
2. Under **Tasks**, click **Add Location**.
3. In the **Add Location Wizard**, click **Next**.
4. Type a name for the location, optionally add a description of it, and then click **Next**.
5. In the list box, select **Client can connect to management server**, and then click **Next**.
6. Click **Finish**.
7. Click **OK**.
8. Under **Tasks**, click **Manage Locations**, and then select the location you created.
9. Beside **Switch to this location when**, click **Add**, and then select **Criteria with AND relationship**.
10. In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.
11. Click **If the client computer does not use the network connection type specified below**.
12. In the bottom list box, select the name of the VPN client that your organization uses, and then click **OK**.
13. Click **Add** and then click **Criteria with AND relationship**.
14. In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.
15. Click **If the client computer uses the network connection type specified below**.
16. In the bottom list box, select **Ethernet**, and then click **OK**.
17. Click **OK** to exit the Manage Locations dialog box.

**To set up the office location for the clients that are logged on over a wireless connection**

1. On the **Clients** page, select the group for which you want to add a location.
2. Under **Tasks**, click **Add Location**.
3. In the **Add Location Wizard**, click **Next**.
4. Type a name for the location, optionally add a description of it, and then click **Next**.
5. In the list box, click **Client can connect to management server**, and then click **Next**.
6. Click **Finish**.



- 
7. Click **OK**.
  8. Under Tasks, click **Manage Locations**, and then select the location that you created.
  9. Beside Switch to this location when, click **Add**, and then click **Criteria with AND relationship**.
  10. In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.
  11. Click **If the client computer does not use the network connection type specified below**.
  12. In the bottom list box, select the name of the VPN client that your organization uses, and then click **OK**.
  13. Click **Add**, and then click **Criteria with AND relationship**.
  14. In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.
  15. Click **If the client computer does not use the network connection type specified below**.
  16. In the bottom list box, click **Ethernet**, and then click **OK**.
  17. Click **Add**, and then click **Criteria with AND relationship**.
  18. In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.
  19. Click **If the client computer uses the network connection type specified below**.
  20. In the bottom list box, click **Wireless**, and then click **OK**.
  21. Click **OK** to exit the **Manage Locations** dialog box.

[Setting up Scenario One location awareness conditions](#)

[Managing remote clients](#)

## Configuring communication settings for a location

By default, you configure communication settings between the management server and the client at the level of the group. However, you can also configure these settings for individual locations in a group. For example, you can use a separate management server for a location where the client computers connect through the VPN. To minimize the number of clients that connect to the management server at the same time, you can specify a different heartbeat for each location.

You can configure the following communication settings for locations:

- The control mode in which the clients run.
- The management server list that the clients use.
- The download mode in which the clients run.
- Whether to collect a list of all the applications that are executed on clients and send the list to the management server.
- The heartbeat interval that clients use for downloads.
- Whether the management server randomizes content downloads from the default management server or a Group Update Provider.

### NOTE

Only some of these settings can be configured for Mac clients.

To configure communication settings for a location

- 
1. In the console, click **Clients**.
  2. On the **Clients** page, select a group.
  3. On the **Policies** tab, under **Location-specific Policies and Settings**, under a location, expand **Location-specific Settings**.
  4. To the right of **Communications Settings**, click **Tasks**, and then uncheck **Use Group Communications Settings**.
  5. Click **Tasks** again, and then click **Edit Settings**.
  6. In the **Communications Settings for location name** dialog box, modify the settings for the specified location only.
  7. Click **OK**.

[Updating policies and content on the client using push mode or pull mode](#)

[Managing locations for remote clients](#)

[Managing groups of clients](#)

## About strengthening your security policies for remote clients

**When you manage remote users, you essentially take one of the following positions:**

- Leave the default policies in place, so that you do not impede remote users in the use of their computers.
- Strengthen your default security policies to provide more protection for your network, even if it restricts what remote users can do.

In most situations, the best practice is to strengthen your security policies for remote clients.

Policies may be created as shared or unshared and assigned either to groups or to locations. A shared policy is one that applies to any group and location and can be inherited. A non-shared policy is one that only applies to a specific location in a group. Typically, it is considered a best practice to create shared policies because it makes it easier to change policies in multiple groups and locations. However, when you need unique location-specific policies, you need to create them as non-shared policies or convert them to non-shared policies.

[Managing remote clients](#)

## Best practices for Firewall policy settings for remote clients

[Firewall policy best practices](#) describes scenarios and best-practice recommendations.

**Table 68: Firewall policy best practices**

Scenario	Recommendation
Remote location where users log on without a VPN	<ul style="list-style-type: none"><li>Assign the strictest security policies to clients that log on remotely without using a VPN.</li><li>Enable NetBIOS protection.</li></ul> <p><b>Note:</b> Do not enable NetBIOS protection for the location where a remote client is logged on to the corporate network through a VPN. This rule is appropriate only when remote clients are connected to the Internet, not to the corporate network.</p> <ul style="list-style-type: none"><li>Block all local TCP traffic on the NetBIOS ports 135, 139, and 445 to increase security.</li></ul>
Remote location where users log on through a VPN	<ul style="list-style-type: none"><li>Leave as-is all the rules that block traffic on all adapters. Do not change those rules.</li><li>Leave as-is the rule that allows VPN traffic on all adapters. Do not change that rule.</li><li>Change the Adapter column from All Adapters to the name of the VPN adapter that you use for all rules that use the action Allow.</li><li>Enable the rule that blocks all other traffic.</li></ul> <p><b>Note:</b> You need to make all of these changes if you want to avoid the possibility of split tunneling through the VPN.</p>
Office locations where users log on through Ethernet or wireless connections	Use your default Firewall policy. For the wireless connection, ensure that the rule to allow wireless EAPOL is enabled. 802.1x uses the Extensible Authentication Protocol over LAN (EAPOL) for connection authentication.

[Creating a firewall policy](#)

[Enabling communications for network services instead of adding a rule](#)

## About turning on notifications for remote clients

**For your remote clients that are not logged on over VPN, it is a best practice to turn on client notifications for the following situations:**

- Intrusion detections  
You can turn on these notifications by using the location-specific server or, you can select the **Mixed control** option in the **Client User Interface Control Settings**. You can customize the settings on the **Client User Interface Settings** tab.
- Virus and security risks  
You can turn on these notifications in the Virus and Spyware Protection policy.

Turning on notifications helps to ensure that remote users are aware when a security problem occurs.

[Managing remote clients](#)

## About monitoring remote clients from the management server

Notifications and logs are essential to maintain a secure environment. In general, you should monitor your remote clients in the same way that you monitor your other clients. You should always check to see that your protections are up to date and that your network is not currently under attack. If your network is under attack, then you want to find out who is behind the attack and how they attacked.

Your Home page preference settings determine the time period for which Symantec Endpoint Protection Manager displays data. By default, the data on the Home page represents only the clients that connected in the past 12 hours. If you have many clients that are frequently offline, your best monitoring option is to go to the logs and reports. In the logs and reports, you can filter the data to include offline clients.

Even if you restrict some of the client log data that mobile clients upload, you can check the following displays.

**Table 69: Displays to monitor remote client security**

Display	Description
<b>Home &gt; Endpoint Status</b>	Displays whether the content is up to date or to see if any of the protections are turned off. <b>You can check the following status conditions:</b> <ul style="list-style-type: none"><li>• Content dates and version numbers</li><li>• Client connections</li><li>• Enabled and disabled protections</li></ul> You can click <b>Details</b> to see the status for each client.
<b>Home &gt; Security Status</b>	Displays the system security overview. View the <b>Virus and Risks Activity Summary</b> to see if your network is under attack. You can click <b>Details</b> to see the status for each security protection technology.
<b>Home &gt; Virus and Risks Activity Summary</b>	Displays the detected virus and risk activity, and the actions taken, such as cleaned, blocked, or quarantined.
<b>Monitors &gt; Summary Type &gt; Network Threat Protection</b>	Displays the information about attack types and sources.

[Managing remote clients](#)

[Monitoring roaming Symantec Endpoint Protection clients from the cloud console](#)

## Monitoring roaming Symantec Endpoint Protection clients from the cloud console

Roaming Symantec Endpoint Protection clients are the clients that intermittently connect to the management server. Roaming clients access the Internet at different locations, such as airports, hotels, or at other companies, where they are at higher risk. Symantec Endpoint Protection Manager provides on and off-network protection for these client computers using location awareness.

In 14.1 and earlier, roaming clients send critical events to the management server only when they are connected. As of 14.2, roaming clients automatically send critical events to the cloud console when the clients cannot connect to the management server. After the roaming client reconnects to the management server, the clients send any new critical events on the management server. The client is also no longer considered to be roaming.

Use the list of critical events as a way to strengthen the security policies on the Symantec Endpoint Protection Manager. For example, suppose Employee1's client has a higher number of denial-of-service attacks when Employee1 is located in a particular hotel. Therefore, you can create a location for that hotel and enable denial of service detections in the Firewall policy.

[What are the critical events that the cloud portal displays?](#)

[About monitoring remote clients from the management server](#)

[Location awareness best practices for Endpoint Protection](#)

### Finding roaming clients and critical events

To find out which clients are roaming, look for the following items:

- Whether the device is connected directly to the cloud console and not the management server.
- The location as defined in the Symantec Endpoint Protection Manager location awareness policy
- The external IP address of the client.

To find roaming clients and critical events

- 
1. In the cloud console, go to **Alerts and Events**.
  2. On the **Security Events** tab, under **Connection Type**, click **Cloud** to display the events that the client sends to the cloud console.  
To display events that the management server sends, click **Symantec Endpoint Protection Manager**.
  3. Under **Severity**, click **Critical**.  
The cloud console filters and displays only the critical security events that the roaming clients detected.
  4. To find the location and external IP address, select the device and look for the Device Location entry.

### **What are the critical events that the cloud console displays?**

The roaming client uploads the following security events to the cloud console:

- Port scan events
- Mac spoofing
- Denial of service
- Canary
- IPS
- Deception
- Memory Exploit Mitigation
- Host Integrity compliance

The roaming client uploads the following security events to the cloud console:

- Antivirus
- SONAR

## **Managing administrator accounts**

You can use administrator accounts to manage Symantec Endpoint Protection Manager datacenters. Administrators log on to Symantec Endpoint Protection Manager to change policy settings, manage groups, run reports, and install client software, as well as other management tasks.

The default account is a system administrator account, which provides access to all features. You can also add a more limited administrator account, for administrators who need to perform a subset of tasks.

For a small company, you may only need one administrator and one domain. For a large company with multiple sites and Windows domains, you most likely need multiple administrators, some of whom have more access rights than others. You may also need to add multiple domains within Symantec Endpoint Protection Manager.

You manage domains and administrator accounts and their passwords on the **Admin** page.

**Table 70: Account administration**

Task	Description
Decide whether to add multiple domains	Decide whether to add domains. <a href="#">About domains</a> <a href="#">Adding a domain</a> <a href="#">Switching to the current domain</a>
Add administrator accounts	Add accounts for administrators who need access to the Symantec Endpoint Protection Manager console. 1. Add the types of administrator accounts that you need, and the level of access rights. <a href="#">About administrator accounts and access rights</a> <a href="#">Adding an administrator account and setting access rights</a> 2. Choose a method to authenticate administrator for when they log on to Symantec Endpoint Protection Manager (optional). By default, the Symantec Endpoint Protection Manager database authenticates the administrator's credentials. <a href="#">Choosing the authentication method for administrator accounts</a>
Unlock or lock an administrator account	By default, Symantec Endpoint Protection Manager locks out an administrator after a user tries to log on to Symantec Endpoint Protection Manager using the administrator account too many times. You can configure these settings to increase the number of tries or time the administrator is locked out. If an administrator is locked out of their account, they must wait the specified time before logging on again. You cannot unlock an account during the lockout interval. <a href="#">Unlocking an administrator's account after too many logon attempts</a>
Change and reset lost passwords	<ul style="list-style-type: none"> <li>Change the password for your account or another administrator's account. <a href="#">Changing the password for an administrator account or the default database</a></li> <li>Reset a lost password using the <b>Forgot your password?</b> link that appears on the management server logon screen. The administrator receives an email that contains a link to activate a temporary password. <a href="#">Resetting a forgotten Symantec Endpoint Protection Manager password</a> <a href="#">Displaying the Forgot your password? link so that administrators can reset lost passwords</a></li> <li>Allow administrators to save their user name and password on the management server logon screen. <a href="#">Displaying the Remember my user name and check boxes on the logon screen</a></li> <li>Force the administrator's logon password to expire after a certain number of days. <a href="#">Displaying the Remember my user name and check boxes on the logon screen</a></li> </ul>
Configure logon options for Symantec Endpoint Protection Manager	You can configure the following logon options for each type of administrator: <ul style="list-style-type: none"> <li>Display a message for administrators to read before they log on. <a href="#">Displaying a message for administrators to see before logging on to the Symantec Endpoint Protection Manager console</a></li> <li>Allow or block log on access to the management console, so that certain administrators can, or cannot, log on remotely. <a href="#">Granting or blocking access to remote Symantec Endpoint Protection Manager consoles</a></li> <li>Changing how long an administrator can stay logged on to the management server. <a href="#">Changing the timeout period for staying logged on to the Symantec Endpoint Protection Manager console</a> <a href="#">Logging on to the Symantec Endpoint Protection Manager console</a></li> </ul>

## About administrator accounts and access rights

When you install the Symantec Endpoint Protection Manager, a default system administrator account is created, called `admin`. The system administrator account gives an administrator access to all the features in Symantec Endpoint Protection Manager.

To help you manage security, you can add additional system administrator accounts, domain administrator accounts, and limited administrator accounts. Domain administrators and limited administrators have access to a subset of Symantec Endpoint Protection Manager features.

You choose which accounts you need based on the types of roles and access rights you need in your company. For example, a large company may use the following types of roles:

- An administrator who installs the management server and the client installation packages. After the product is installed, an administrator in charge of operations takes over. These administrators are most likely system administrators.
- An operations administrator maintains the servers, databases, and installs patches. If you have a single domain, the operations administrator could be a domain administrator who is fully authorized to manage sites.
- An antivirus administrator, who creates and maintains the Virus and Spyware Protection policies and LiveUpdate policies on the clients. This administrator is most likely to be a limited administrator.
- A desktop administrator, who is in charge of security and creates and maintains the Firewall policies and Intrusion Prevention policies for the clients. This administrator is most likely to be a domain administrator.
- A help desk administrator, who creates reports and has read-only access to the policies. The antivirus administrator and desktop administrator read the reports that the help desk administrator sends. The help desk administrator is most likely to be a limited administrator who is granted reporting rights and policy rights.

**Table 71: Administrator roles and responsibilities**

Administrator role	Responsibilities
<b>System administrator</b>	<p>System administrators can log on to the Symantec Endpoint Protection Manager console with complete, unrestricted access to all features and tasks.</p> <p>A system administrator can create and manage other system administrator accounts, domain administrator accounts, and limited administrator accounts.</p> <p><b>A system administrator can perform the following tasks:</b></p> <ul style="list-style-type: none"> <li>• Manage all domains.</li> <li>• Administer licenses.</li> <li>• View and manage all console settings.</li> <li>• Manage the databases and management servers.</li> </ul>
Administrator	<p>Administrators are domain administrators who can view and manage a single domain. A domain administrator has the same privileges as a system administrator, but for a single domain only.</p> <p>By default, the domain administrator has full system administrator rights to manage a domain, but not a site. You must explicitly grant site rights within a single domain. Domain administrators can modify the site rights of other administrators and limited administrators, though they cannot modify the site rights for themselves.</p> <p>A domain administrator can perform the following tasks:</p> <ul style="list-style-type: none"> <li>• Create and manage administrator accounts and limited administrator accounts within a single domain. Domain administrators cannot modify their own site rights. System administrators must perform this function.</li> <li>• Run reports, manage sites, and reset passwords.</li> <li>• Cannot administer licenses. Only system administrators can administer licenses.</li> </ul> <p><a href="#">About domains</a></p>
<b>Limited administrator</b>	<p>Limited administrators can log on to the Symantec Endpoint Protection Manager console with restricted access. Limited administrators do not have access rights by default. A system administrator role must explicitly grant access rights to allow a limited administrator to perform tasks.</p> <p>Parts of the management server user interface are not available to limited administrators when you restrict access rights. For example:</p> <ul style="list-style-type: none"> <li>• Limited administrators without reporting rights cannot view the <b>Home</b>, <b>Monitors</b>, or <b>Reports</b> pages.</li> <li>• Limited administrators without policy rights cannot view or modify the policy. In addition, they cannot apply, replace, or withdraw a policy.</li> </ul>

[Adding an administrator account and setting access rights](#)

[Managing administrator accounts](#)

---

## Adding an administrator account and setting access rights

As a system administrator, you can add another system administrator, administrator, or limited administrator. As an administrator within a domain, you can add other administrators with access rights equal to or less restrictive than your own. Administrators can add limited administrators and configure their access rights.

To add an administrator account

1. In the console, click **Admin > Administrators**.
2. Under **Tasks**, click **Add an administrator**.
3. In the **Add Administrator** dialog box, on the **General** tab, enter the user name and email address.
4. On the **Access Rights** tab, specify the type of administrator account.

If you add an account for a limited administrator, you must also specify the administrator's access rights. Limited administrator accounts that are not granted any access rights are created in a disabled state and the limited administrator cannot log on to the management server.

[About administrator accounts and access rights](#)

5. On the **Authentication** tab, under **Symantec Endpoint Protection Manager Authentication**, type the password the administrator should use to log on.

When the administrator logs on to the Symantec Endpoint Protection Manager, Symantec Endpoint Protection Manager verifies with the database that the user name and password are correct.

[Choosing the authentication method for administrator accounts](#)

6. Click **OK**.

## Choosing the authentication method for administrator accounts

You can choose from several authentication methods that the management server uses to check administrators' credentials before they log on.

For the third-party authentication methods, Symantec Endpoint Protection Manager has an entry in the database for the administrator account, but the third-party server validates the user name and password.

**Table 72: Authentication methods**

Type	When to use
Symantec Endpoint Protection Manager authentication (default)	Authenticates the administrators with the administrator's user name and password that are stored in the Symantec Endpoint Protection Manager database. When the administrator logs on to the management server, the management server verifies with the database that the user name and password are correct. You can display the <b>Password never expires</b> option so that an administrator's account does not expire. <a href="#">Enabling Symantec Endpoint Protection Manager logon passwords to never expire</a>
Two-factor authentication	Authenticates the administrators with Symantec VIP authentication on their smartphone. Administrators provide a unique, one-time verification code when they log on, in addition to a password. For this option to be available, you must first add the appropriate PKCS keystore file and keystore's password. <a href="#">Configuring two-factor authentication with Symantec VIP</a>
RSA SecurID authentication	Authenticates the administrators by a using RSA SecurID token (not software RSA tokens), RSA SecurID card, or RSA keypad card (not RSA smart cards). To authenticate administrators who use an RSA SecurID mechanism, first install the RSA Authentication Manager server and enable encrypted authentication for RSA SecurID. <a href="#">Using RSA SecurID authentication with Symantec Endpoint Protection Manager</a>



Type	When to use
Directory server authentication	<p>Authenticates the administrators with an LDAP server or the Microsoft Active Directory server. To authenticate administrators using an Active Directory or LDAP directory server, you need to set up an account on the directory server. You must also establish a connection between the directory server and Symantec Endpoint Protection Manager. If you do not establish a connection, you cannot import users from an Active Directory server or synchronize with it.</p> <p><b>Note:</b> Synchronization is only possible for Active Directory Servers. Synchronization with LDAP servers is not supported.</p> <p><a href="#">Connecting Symantec Endpoint Protection Manager to a directory server</a>  <a href="#">Checking the authentication to a directory server</a></p>
Smart card authentication	<p>Authenticates the administrators who work as civilians or military personnel in U.S. Federal Agencies and who must use a PIV card or CAC to log on.</p> <p><a href="#">Configuring Symantec Endpoint Protection Manager to authenticate administrators who log on with smart cards</a></p>

To choose an authentication method for administrator accounts

1. Add an administrator account.

[Adding an administrator account and setting access rights](#)

2. On the **Authentication** tab, select the authentication method if you do not want to use **Symantec Endpoint Protection Manager Authentication** (default).
3. Click **OK**.
4. In the **Confirm Change** dialog box, type the password that you use to log on to Symantec Endpoint Protection Manager, and then click **OK**.

When you switch between authentication methods, you must type the administrator account's password.

## Using RSA SecurID authentication with Symantec Endpoint Protection Manager

### NOTE

In an IPv6 environment, you must install and enable the IPv4 stack on the Symantec Endpoint Protection Manager server to use RSA SecurID authentication.

(IPv6 networking is supported as of version 14.2.)

### Configure RSA SecurID to authenticate Symantec Endpoint Protection Manager administrators

If you want to authenticate administrators who use the Symantec Endpoint Protection Manager with RSA SecurID, you must first enable encrypted authentication by configuring a connection to an RSA Authentication Manager server.

1. Install an RSA Authentication Manager server, if necessary. Use RSA Authentication Manager 8.1.
2. Install and properly configure the RSA Authentication Agent on the Symantec Endpoint Protection Manager server to connect to the RSA server. Use RSA Authentication Agent 7.x.
3. Ensure that the Symantec Endpoint Protection Manager server registers as a valid host on the RSA Authentication Manager server.
4. Ensure that the `sdconf.rec` file on the RSA Authentication Manager server is accessible on the network.
5. Assign a synchronized SecurID card or key fob to a management server account; activate the logon name on the RSA Authentication Manager server.
6. Ensure that the administrator has the RSA PIN or password available.

Symantec supports the following types of RSA logons:

- 
- RSA SecurID token (not software RSA tokens)
  - RSA SecurID card
  - RSA keypad card (not RSA smart cards)

To log on to the management server with the RSA SecurID, an administrator needs a logon name, the token (hardware), and a PIN.

### **Install the RSA Authentication Agent and configure the Symantec Endpoint Protection Manager server to use RSA SecurID authentication**

To use RSA SecurID with Symantec Endpoint Protection Manager, you must install the RSA Authentication Agent on the Symantec Endpoint Protection Manager server and configure it as a SecurID Authentication client.

#### **To install the RSA Authentication Agent**

1. Install the software for the RSA Authentication Agent on the Symantec Endpoint Protection Manager server. You can install the software by running the Windows .msi file from the RSA Authentication Agent installation file.
2. Copy the `sdconf.rec` file from the RSA Authentication server to the Symantec Endpoint Protection Manager server. For earlier versions of RSA Authentication Agent, copy `nodesecret.rec`, `sdconf.rec`, and `agent_nsload.exe`.

#### **To configure the Symantec Endpoint Protection Manager server to use RSA SecurID authentication**

1. Log on to the Symantec Endpoint Protection Manager console, and then click **Admin > Servers**.
2. Under **Servers**, under **Local Site**, click the management server.
3. Under **Tasks**, click **Configure SecurID authentication**.
4. In the **Welcome to the Configure SecurID Authentication Wizard** panel, click **Next**.
5. In the **Qualification** panel of the **Configure SecurID Authentication Wizard** panel, read the prerequisites and verify that you meet them all.
6. Click **Next**.
7. In the **Upload RSA File** panel of the **Configure SecurID Authentication Wizard** panel, browse for the folder in which the `sdconf.rec` file resides.  
You can also type the path name.
8. Click **Next**, and then click **Test** to test your configuration.
9. In the **Test Configuration** dialog box, type the user name and password for your SecurID, and then click **Test**.  
It now authenticates successfully.

#### **Add Symantec Endpoint Protection Manager administrators who use RSA SecurID authentication**

1. Add an administrator account.  
[Adding an administrator account and setting access rights](#)
2. On the **Authentication** tab, click RSA SecurID Authentication.  
If this option is unavailable, review the configuration guidelines.  
[Configure RSA SecurID to authenticate](#)
3. Click **OK**.  
You can also change an existing administrator account to use RSA SecurID authentication, though this practice is not recommended, especially for default administrator account, admin. If you provide invalid information when you edit an existing user, it is more difficult to recover that user.  
However, if you modify an existing administrator account, in the **Confirm Change** dialog box, type the password that you use to log on to Symantec Endpoint Protection Manager, and then click **OK**.  
When you switch between authentication methods, you must type the administrator account's password.  
[Choosing the authentication method for administrator accounts](#)

---

## Configuring two-factor authentication with Symantec VIP

If you use Symantec VIP two-factor authentication in your environment, you can configure Symantec Endpoint Protection Manager administrators to authenticate with it.

Two-factor authentication adds an extra layer of security to the logon process. When two-factor authentication is enabled, you must provide a unique, one-time verification code when you log on, in addition to a password. You can receive the code by voice, text, or with the free Symantec VIP Access app. This app is recommended because it is the most secure and it is easy to use. For a quick overview of Symantec VIP, see:

[Symantec VIP: Enterprise-grade authentication made easy for everyone](#)

You manage the individual two-factor authentication settings for each individual administrator that uses Symantec Endpoint Protection Manager Authentication. Administrators that authenticate with RSA SecurID or Directory authentication cannot use two-factor authentication.

### NOTE

Two-factor authentication is not supported over IPv6, or in a FIPS-enabled environment.

To configure Symantec Endpoint Protection Manager for two-factor authentication with Symantec VIP

1. In the console, click **Admin > Servers**, and then click the local server name.
2. Under **Tasks**, click **Configure VIP authentication**.
3. Browse to the PKCS keystore file to select it, enter the keystore's password, and then click **OK**.

The certificate automatically propagates to other Symantec Endpoint Protection Manager consoles in the same site without the need for replication. You do not need to manually add the certificate to each Symantec Endpoint Protection Manager on the site.

To propagate the certificate to a Symantec Endpoint Protection Manager on a different site, the sites must be replication partners.

To configure the administrator for two-factor authentication with Symantec VIP

4. Verify that the Symantec Endpoint Protection Manager administrator has a corresponding user name on the Symantec VIP Manager that matches exactly, including case sensitivity. The passwords for the two user names do not have to match.

Consult Symantec VIP Manager documentation for how to configure a user name.

[Symantec VIP Access Manager 3.0 Administrator's Guide](#)

5. In the console, click **Admin > Servers > Administrators**.
6. Select an existing administrator, and then click **Edit the administrator**.

You can also add a new administrator to configure.

7. On the **Authentication** tab, click **Enable two-factor authentication using VIP**.

## Configuring Symantec Endpoint Protection Manager to authenticate administrators who log on with smart cards

In 14.2 or later, administrators who work for US Federal Agencies can log on to Symantec Endpoint Protection Manager using a smart card.

To set up smart card authentication, the administrator needs to perform the following steps:

[Step 1: Configure Symantec Endpoint Protection Manager for smart card authentication](#)

[Step 2: Configure the management server to perform the revocation check \(dark networks only\) \(Optional\)](#)

---

[Step 3: Add an administrator account and register the smart card](#)

[Step 4: Log on to Symantec Endpoint Protection Manager using a smart card](#)

### About smart cards

The United States Federal Agencies now use a software system that allows smart card authentication for the HSPD-12 requirements. A U.S. Federal smart card contains the necessary data for the cardholder to be granted access to Federal facilities and information systems. This access ensures appropriate levels of security for all applicable Federal applications.

Some Windows client computers or workstations already have PIV or CAC readers built into the keyboards.

Symantec Endpoint Protection Manager authenticates administrators who use the following types of smart cards:

- Personal identity verification (PIV) card (for civilians)
- Common Access Card (CAC) (for military personnel)
- In FIPS mode: Symantec Endpoint Protection Manager does not support smart cards that are signed using ECDSA and RSASSA-PSS.
- In non-FIPS mode: Symantec Endpoint Protection Manager does not support smart cards that are signed using RSASSA-PSS.

See: [HSPD-12](#)

### Step 1: Configure Symantec Endpoint Protection Manager for smart card authentication

This step validates that the card certificate is issued by the correct authority. Then, at the point that the administrator logs on, the management server reads the smart card's certificate and validates it against these CA certificates.

To validate a certificate file, the management server checks that the certificate file is not listed in a certificate revocation list (CRL) on the Internet.

Make sure that all the root files and intermediate files are present on the administrators' computer, or else they cannot log on.

#### To configure Symantec Endpoint Protection Manager for smart card authentication

1. In the console, click **Admin > Servers**, and select the local management server name.
2. Under **Tasks**, click **Configure Smart Card Authentication**.
3. In the **Specify the paths for the root and/or intermediate certificate files** text box, browse to one or more certificate files, and then click **OK**.

Select all the certificate files you need to check for revocation. To select multiple files, press **Ctrl**.

**Optional:** If the management server that the administrator logs on to cannot access the Internet, in the **Specify the paths for the certificate revocation lists** text box, add a .crl or a .pem file. You must also perform the following task on these management servers. [Step 2: Configure the management server to perform the revocation check \(dark networks only\)](#)

4. Click **OK**.
5. If the administrator logs on to Symantec Endpoint Protection Manager remotely with the web console, they must restart the Symantec Endpoint Protection Manager service and the Symantec Endpoint Protection Manager Web service.

[Stopping and starting the management server service](#)

### Step 2 (Optional): Configure the management server to perform the revocation check (Required for dark networks)

If a management server does not have Internet access, you must configure it to check for the CRL file on the management server computer instead. Without this check, administrators can still log on, but the management server cannot check the CRL file, which can cause security issues.

---

## To configure the management server to perform the revocation check (dark networks only)

1. On this management server, open the following file: `Symantec Endpoint Protection Manager installation path\tomcat\etc\conf.properties`
2. In the `conf.properties` file, add `smartcard.cert.revocation.ocsp.crl.dp.enabled=false` and save the file.
3. Restart the management server service.

### [Stopping and starting the management server service](#)

## Step 3 (Optional): Configure the management server to perform the revocation check (Required for dark networks)

This step authenticates the administrators as the user of the smart card by setting up PIV authentication. PIV authentication requires a certificate and key pair that is used to verify that the PIV credential was issued by an authorized entity, has not expired, and has not been revoked. The PIV credential also identifies the administrator the same individual it was issued to.

This step also ensures that users only need to enter their user name, insert the card, and type the smart card pin to log on to Symantec Endpoint Protection Manager. They do not need to enter a Symantec Endpoint Protection Manager password.

Smart card authentication is not supported over IPv6.

1. In the console, click **Admin > Servers > Administrators**.
2. Add a new administrator or edit an existing administrator.  
[Adding an administrator account and setting access rights](#)
3. On the **Authentication** tab, click **Enable smart card authentication**.
4. Browse to the authentication certificate file for the PIV card or CAC for that administrator, and then click **OK**.
5. In the **Confirm Change** dialog box, type the administrator's password and click **OK**.  
Follow this step for each administrator that uses a smart card to log on to Symantec Endpoint Protection Manager.

## Step 4: Log on to Symantec Endpoint Protection Manager using a smart card

To log on to Symantec Endpoint Protection Manager, the administrator inserts the card into a smart card reader and types a pin number. The smart card must always be inserted into the reader while the smart card administrator is logged on and using the management server. If the administrator removes the smart card, the Symantec Endpoint Protection Manager logs off the administrator within 30 seconds.

The Java console and web console support smart card authentication. The RMM console and the REST API do not support smart card authentication.

### [Logging on to the Symantec Endpoint Protection Manager console](#)

## Troubleshooting and replication

If two sites replicate each other, the site with the most recently configured CA file overwrites the CA file on all other sites.

## Testing directory server authentication for an administrator account

You can check that an Active Directory or LDAP server authenticates the user name and password for an administrator account that you create. The check evaluates whether you added the user name and password correctly, and whether or not the account name exists on the directory server.

You use the same user name and password for an administrator account in Symantec Endpoint Protection Manager as you do in the directory server. When the administrator logs on to the management server, the directory server authenticates the administrator's user name and password. The management server uses the directory server configuration that you added to search for the account on the directory server.

---

You can also check whether an Active Directory or LDAP server authenticates an administrator account with no user name and password. An account with no user name or password is anonymous access. You should create an administrator account with anonymous access so that the administrators are never locked out if the password changes on the directory server.

#### NOTE

In Windows 2003 Active Directory server, anonymous authentication is disabled by default. Therefore, when you add a directory server without a user name to an administrator account and click **Check Account**, an **Account Authentication Failed** error message appears. To work around this issue, create two directory server entries, one for testing, and one for anonymous access. The administrator can still log on to the management server using a valid user name and password.

#### Step 1: Add multiple directory server connections

To make testing easier for anonymous access, add at least two directory server entries. Use one entry to test the authentication, and the second entry to test anonymous access. These entries all use the same directory server with different configurations.

By default, most users reside in CN=Users unless moved to different organizational unit. Users in the LDAP directory server are created under CN=Users, DC=<sampldomain>, DC=local. To find out where a user resides in LDAP, use ADSIEdit.

Use the following information to set up the directory servers for this example:

- CN=John Smith
- OU=test
- DC=<sampldomain>
- DC=local

The example uses the default Active Directory LDAP (389) but can also use Secure LDAP (636).

1. To add the directory server connections to check Active Directory and LDAP server authentication, on the console, click **Admin > Servers**, select the default server, and click **Edit the server properties**.
2. On the **Directory Servers** tab, click **Add**.
3. On the **General** tab, add the following directory server configurations, and then click **OK**.

Directory 1	<ul style="list-style-type: none"><li>• <b>Name:</b> &lt;sampldomain&gt; Active Directory</li><li>• <b>Server Type:</b> Active Directory</li><li>• <b>Server IP Address or Name:</b> server01.&lt;sampldomain&gt;.local</li><li>• <b>User Name:</b> &lt;sampldomain&gt;\administrator</li><li>• <b>Password:</b> &lt;directory server password&gt;</li></ul>
Directory 2	<ul style="list-style-type: none"><li>• <b>Name:</b> &lt;sampldomain&gt; LDAP with User Name</li><li>• <b>Server Type:</b> LDAP</li><li>• <b>Server IP Address or Name:</b> server01.&lt;sampldomain&gt;.local</li><li>• <b>LDAP Port:</b> 389</li><li>• <b>LDAP BaseDN:</b> DC=&lt;sampldomain&gt;, DC=local</li><li>• <b>User Name:</b> &lt;sampldomain&gt;\administrator</li><li>• <b>Password:</b> &lt;directory server password&gt;</li></ul>

Directory 3	<ul style="list-style-type: none"> <li>• <b>Name:</b> &lt;sampldomain&gt; LDAP without User Name</li> <li>• <b>Server Type:</b> LDAP</li> <li>• <b>Server IP Address or Name:</b> server01.&lt;sampldomain&gt;.local</li> <li>• <b>LDAP Port:</b> 389</li> <li>• <b>LDAP BaseDN:</b> &lt;empty&gt; Leave this field empty when you use anonymous access.</li> <li>• <b>User Name:</b> &lt;empty&gt;</li> <li>• <b>Password:</b> &lt;empty&gt; After you click <b>OK</b>, a warning appears. But the directory server is valid. When you try to add a BaseDN without a user name and password, the warning appears.</li> </ul>
-------------	---

## Step 2: Add multiple administrator accounts

You add multiple system administrator accounts. The account for anonymous access does not have a user name or password.

1. To add the administrator accounts using the directory server entries, on the console, click **Admin > Administrators**, and on the **General** tab, add the administrator accounts in the previous step.  
[Adding an administrator account and setting access rights](#)  
[Choosing the authentication method for administrator accounts](#)
2. After you add each administrator account and click the **Check Account** option, you see a message. In some cases, the message appears to invalidate the account information. The administrator can still log on to Symantec Endpoint Protection Manager, however.
3. On the **General** tab, enter the following information:

Administrator 1	<ul style="list-style-type: none"> <li>• <b>Name:</b> &lt;sampldomain&gt; LDAP without User Name</li> <li>• <b>Server Type:</b> LDAP</li> <li>• <b>Server IP Address or Name:</b> server01.&lt;sampldomain&gt;.local</li> <li>• <b>LDAP Port:</b> 389</li> <li>• <b>LDAP BaseDN:</b> &lt;empty&gt; Leave this field empty when you use anonymous access.</li> <li>• <b>User Name:</b> &lt;empty&gt;</li> <li>• <b>Password:</b> &lt;empty&gt; After you click <b>OK</b>, a warning appears. But the directory server is valid. When you try to add a BaseDN without a user name and password, the warning appears.</li> </ul>
Administrator 2	<ul style="list-style-type: none"> <li>• <b>User Name:</b> john</li> <li>• <b>Full Name:</b> John Smith</li> <li>• <b>Email Address:</b> john@&lt;sampldomain&gt;.local</li> <li>• On the <b>Access Rights</b> tab, click <b>System Administrator</b>.</li> <li>• On the <b>Authentication</b> tab, click <b>Directory Authentication</b>. In the <b>Directory Server</b> drop-down list, select &lt;sampldomain&gt; LDAP with User Name. In the <b>Account Name</b> field, type john. Click <b>Check Account</b>. The system administrator john cannot log on into Symantec Endpoint Protection Manager with directory authentication</li> </ul>



Administrator 3	<ul style="list-style-type: none"> <li>• <b>User Name:</b> john</li> <li>• <b>Full Name:</b> John Smith</li> <li>• <b>Email Address:</b> john@&lt;sampldomain&gt;.local</li> <li>• On the <b>Access Rights</b> tab, click <b>System Administrator</b>.</li> <li>• On the <b>Authentication</b> tab, click <b>Directory Authentication</b>.</li> </ul> <p>In the <b>Directory Server</b> drop-down list, select &lt;sampldomain&gt; LDAP with User Name.</p> <p>In the <b>Account Name</b> field, type John Smith.</p> <p>Click <b>Check Account</b>.</p> <p>The system administrator john can log on into Symantec Endpoint Protection Manager with directory authentication.</p>
Administrator 4	<ul style="list-style-type: none"> <li>• <b>User Name:</b> john</li> <li>• <b>Full Name:</b> John Smith</li> <li>• <b>Email Address:</b> john@&lt;sampldomain&gt;.local</li> <li>• On the <b>Access Rights</b> tab, click <b>System Administrator</b>.</li> <li>• On the <b>Authentication</b> tab, click <b>Directory Authentication</b>.</li> </ul> <p>In the <b>Directory Server</b> drop-down list, select &lt;sampldomain&gt; LDAP without User Name.</p> <p>In the <b>Account Name</b> field, type John Smith.</p> <p>Click <b>Check Account</b>.</p> <p>The account authentication fails, but the system administrator John Smith can log on to Symantec Endpoint Protection Manager.</p>

[Connecting Symantec Endpoint Protection Manager to a directory server](#)

## Changing the password for an administrator account or the default database

### Changing the password for an administrator account

You need to change the password for your account or another administrator's account if the password is forgotten, lost, or compromised.

The following rules apply to changing passwords:

- System administrators can change the password for all administrators.
- Domain administrators can change the password for other domain administrators and limited administrators within the same domain.
- Limited administrators can change their own passwords only.

If you change the password to fix an administrator account lockout, the administrator must still wait for the lockout period to expire.

#### NOTE

The password must contain at least 8 characters and fewer than 16 characters. It must include at least one lowercase letter [a-z], one uppercase letter [A-Z], one numeric character [0-9], and one special character such as ["/\ [ ] : ; | = , + \* ? < > ] @. (14.2 or later)

[Unlocking an administrator's account after too many logon attempts](#)

1. In the console, click **Admin > Administrators**.
2. Under **Administrators**, select the administrator account, and then click **Change password**.  
Press **F1** to see the password restrictions.
3. Type both your password and the administrator's new password.
4. Click **Change**.

[Resetting a forgotten Symantec Endpoint Protection Manager](#)

[Displaying the Forgot your password? link so that administrators can reset lost passwords](#)

### Changing the default SQL Server Express database password



---

When you configure the management server and select the default database (Microsoft SQL Server Express or embedded (14.3 MPx and earlier), the password you enter for the default administrator account, `admin`, also becomes the database password. If you change the default administrator's password, the database password does not change automatically. You can change the database password by rerunning the Management Server Configuration Wizard and reconfiguring Symantec Endpoint Protection Manager.

1. On the Windows **Start** menu, navigate to **Symantec Endpoint Protection Manager > Management Server Configuration Wizard**.
2. Click **Reconfigure the management server**, and then click **Next > Next**.  
[Reinstalling or reconfiguring Symantec Endpoint Protection Manager password](#)
3. Click **Default SQL Server Express database > Change the database administrator password**, and type the new password.
4. Follow the instructions in each panel to finish the configuration.

## Resetting a forgotten Symantec Endpoint Protection Manager password

If you have a system administrator account, you can reset your own password and allow other administrators to reset their own passwords.

**To reset a lost password, make sure that the following items are enabled:**

- Administrators can reset their own passwords.  
[Displaying the Forgot your password? link so that administrators can reset lost passwords](#)
- The **Forgot your password?** link is set to appear on the management server logon screen. By default, this link appears.  
[Displaying the Remember my user name and check boxes on the logon screen](#)
- The mail server must be configured so that the mail server sends the notification.  
To troubleshoot Symantec Endpoint Protection Manager email failure, see [Sending test email messages fails in Endpoint Protection Manager console](#).  
[Establishing communication between the management server and email servers](#)

Use this method for the administrator accounts that authenticate by using Symantec Management Server authentication but not by either RSA SecurID authentication or directory authentication.

### NOTE

The password must contain at least 8 characters and fewer than 16 characters. It must include at least one lowercase letter [a-z], one uppercase letter [A-Z], one numeric character [0-9], and one special character ["/ \ [ ] : ; | = , + \* ? < > ].

(As of version 14.2.)

### [Choosing the authentication method for administrator accounts](#)

To reset a forgotten Symantec Endpoint Protection Manager password

1. On the management server computer, click **Start > All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager**.  
By default, the **Forgot your password?** link appears on the management server logon screen.
2. In the **Logon** screen, click **Forgot your password?**
3. In the **Forgot Password** dialog box, type the user name for the account for which to reset the password.

For domain administrators and limited administrators, type the domain name for the account. If you did not set up domains, leave the domain field blank.

---

#### 4. Click **Temporary Password**.

The administrator receives an email that contains a link to activate a temporary password. An administrator can request a temporary password from the management console only once per minute. For security reasons, the management server does not verify the entries.

#### 5. The administrator must change the temporary password immediately after logging on.

To verify whether the administrator successfully reset the password, check that the administrator received the email message.

### [Changing the password for an administrator account or the default database](#)

#### **When you cannot reset your password**

If you cannot recover your administrator password with the **Forgot your password?** functionality, Symantec cannot assist with the recovery of your password. You must reconfigure the Symantec Endpoint Protection Manager and database without a database backup. This procedure overwrites the previous management server and database settings and enables you to recreate a new password. Therefore, it is critical that you configure your email settings correctly when you set up the management server and when you audit administrator account information.

### [Restoring the database](#)

### [Reinstalling or reconfiguring Symantec Endpoint Protection Manager.](#)

## **Displaying the Forgot your password? link so that administrators can reset lost passwords**

If you have a system administrator account, you can enable other administrators to reset their forgotten passwords. You enable a **Forgot your password?** link on the Symantec Endpoint Protection Manager logon screen so that administrators can request a temporary password.

To allow administrators to reset forgotten passwords

1. In the console, click **Admin**.
2. On the **Admin** page, click **Servers**.
3. Under **Servers**, select the local site.

You control this setting only for the local site.

4. Click **Edit Site Properties**.
5. On the **Passwords** tab, check **Allow administrators to reset the passwords**.
6. Click **OK**.

### [Resetting a forgotten Symantec Endpoint Protection Manager password](#)

### [Displaying the Remember my user name and check boxes on the logon screen](#)

## **Enabling Symantec Endpoint Protection Manager logon passwords to never expire**

If you use Symantec Endpoint Protection Manager authentication, the default option for passwords is set to expire after 60 days.

You can display an option for administrators to use a password that never expires. This option is disabled by default to increase security, so you must enable it first. After you enable the option, the option appears on the **Authentication** tab for an administrator account.

To enable Symantec Endpoint Protection Manager logon passwords to never expire

- 
1. In the console, click **Admin**.
  2. On the **Admin** page, click **Domains**.
  3. Under **Domains**, select the domain for which to allow administrators to save logon credentials.
  4. Click **Edit Domain Properties**.
  5. On the **Passwords** tab, click **Allow never expiring passwords for administrators**.
  6. Click **OK**.
  7. Click **Admin > Administrators**, and open the administrator account.
  8. On the **Authentication** tab, click **Password never expires**, and then click **OK**.

[Resetting a forgotten Symantec Endpoint Protection Manager password](#)

[Unlocking an administrator's account after too many logon attempts](#)

## Displaying a message for administrators to see before logging on to the Symantec Endpoint Protection Manager console

You can create and display a customizable message that all administrators see before they can log on to the console. The main purpose is to display a legal notice to tell the administrators that they are about to log on to a proprietary computer.

The message appears in the console after administrators type their user name and password and click **Log On**. After administrators have read the message, they can acknowledge the notice and click **OK**, which logs on the administrators. If administrators click **Cancel**, the logon process is canceled, and the administrator is taken back to the logon window.

The message also appears if the administrator runs the reporting functions from a standalone web browser that is connected to the management server.

To display a message for administrators to see before logging on to the Symantec Endpoint Protection Manager console

1. In the console, click **Admin**, and then click **Domains**.
2. Select the domain for which you want to add a logon banner.
3. Under **Tasks**, click **Edit Domain Properties**.
4. On the **Logon Banner** tab, check **Provide a legal notice to administrators when they log on to Symantec Endpoint Protection Manager**.
5. Type the banner title and text.  
Click **Help** for more information.
6. Click **OK**.

[Adding an administrator account and setting access rights](#)

## Displaying the Remember my user name and Remember my password check boxes on the logon screen

A system administrator can enable the **Remember my user name** and **Remember my password** check boxes to appear on the Symantec Endpoint Protection Manager logon screen for another administrator account. The administrator's user name and password are prepopulated on the logon screen.

To display the **Remember my user name** and **Remember my password** check boxes on the logon screen

- 
1. In the console, click **Admin**.
  2. On the **Admin** page, click **Domains**.
  3. Under **Domains**, select the domain for which to allow administrators to save logon credentials.
  4. Click **Edit Domain Properties**.
  5. On the **Passwords** tab, check **Allow users to save credentials when logging on**.
  6. Click **OK**.

[Resetting a forgotten Symantec Endpoint Protection Manager password](#)

## Granting or blocking access to remote Symantec Endpoint Protection Manager consoles

By default, all consoles are granted access. Administrators can log on to the main console locally or remotely from any computer on the network.

You can secure a management console from remote connections by denying access to certain computers.

**You may want to grant or deny access from the following types of users or computers:**

- You should deny access to anyone on the Internet. Otherwise, the console is exposed to Internet attacks.
- You should deny access to limited administrators who use consoles on a different network than the network they manage.
- You should grant access to system administrators and IT administrators.
- You should grant access to lab computers, such as a computer that is used for testing.

In addition to globally granting or denying access, you can specify exceptions by IP address. If you grant access to all remote consoles, the management server denies access to the exceptions. Conversely, if you deny access to all remote consoles, you automatically grant access to the exceptions. When you create an exception, the computer that you specified must have a static IP address. You can also create an exception for a group of computers by specifying a subnet mask. For example, you may want to grant access in all areas that you manage. However, you may want to deny access to a console that is located in a public area.

To grant or deny access to a remote console

1. In the console, click **Admin**, and then click **Servers**.
2. Under **Servers**, select the server for which you want to change the remote console access permission.
3. Under **Tasks**, click **Edit the server properties**.
4. On the **General** tab, click **Granted Access** or **Denied Access**.
5. If you want to specify IP addresses of the computers that are exempt from this console access permission, click **Add**.  
Computers that you add become exceptions. If you click **Granted Access**, the computers that you specify are denied access. If you click **Denied Access**, the computers that you specify are granted access. You can create an exception for a single computer or a group of computers.
6. In the **Deny Console Access** dialog box, click one of the following options:
  - **Single Computer**  
For one computer, type the IP address.
  - **Group of Computers**  
For several computers, type both the IP address and the subnet mask for the group.
7. Click **OK**.

The computers now appear in the exceptions list. For each IP address and mask, its permission status appears.

---

If you change **Granted Access** to **Denied Access** or vice versa, all exceptions change as well. If you have created exceptions to deny access, they now have access.

8. Click **Edit All** to change the IP addresses or host names of those computers that appear on the exceptions list.

The **IP Address Editor** appears. The **IP Address Editor** is a text editor that lets you edit IP addresses and subnet masks.

9. Click **OK**.

10. When you finish adding exceptions to the list or editing the list, click **OK**.

[Adding an administrator account and setting access rights](#)

[Logging on to the Symantec Endpoint Protection Manager console](#)

## Unlocking an administrator's account after too many logon attempts

Symantec Endpoint Protection Manager locks out an administrator for a certain length of time after a number of unsuccessful logon attempts. By default, the management server locks out an administrator for 15 minutes after five failed attempts.

You cannot unlock the administrator account without waiting for the specified period of time to pass. However, you can disable the administrator account from locking, though this action does not unlock the account. You can also change the number of unsuccessful logon attempts and wait the time that is permitted before the account is locked. A password change does not reset or otherwise affect the lockout interval.

For added security after the first lockout the lockout interval doubles with each additional lockout. Symantec Endpoint Protection Manager reinstates the original lockout interval after a successful logon occurs or after 24 hours pass since the first lockout. For example, if the original lockout interval is 15 minutes, the second lockout triggers a 30-minute lockout interval. The third lockout triggers a 60-minute lockout interval. If the first lockout occurs at 2:00 P.M. on Thursday, then the 24-hour period ends 2:00 P.M. Friday, and Symantec Endpoint Protection Manager resets the lockout interval to 15 minutes.

To unlock an administrator's account after too many logon attempts

1. In the console, click **Admin > Administrators**.
2. Under **Administrators**, select the administrator account that is locked.
3. Under **Tasks**, click **Edit the administrator**.
4. On the **General** tab, uncheck **Lock the account after the specified number of unsuccessful logon attempts**.

[Resetting a forgotten Symantec Endpoint Protection Manager password](#)

[Changing the password for an administrator account or the default database](#)

[Enabling Symantec Endpoint Protection Manager logon passwords to never expire](#)

## Changing the timeout period for staying logged on to the Symantec Endpoint Protection Manager console

To help protect Symantec Endpoint Protection Manager, the console requires you to enter your user name and password again after one hour. To increase security, you can decrease the timeout period before you must log on to the management console again.

This logon timeout period applies to when you log on to the management console locally or through the remote Java console. The logon timeout period for the remote web console is based on the shortest timeout value that you define. For

---

example, you set the **Site Properties** settings to 60 minutes, the Apache settings to 30 minutes, and the browser settings to 10 minutes. The console then times out after 10 minutes.

1. To change the timeout period for staying logged on to the Symantec Endpoint Protection Manager local or remote Java console, in the console, click **Admin**, and then click **Servers**.
2. Click **Local Site** or a remote site and click **Edit Site Properties**.
3. On the **General** tab, click the **Console Timeout** drop-down list and select one of the available options for length of time.
4. Click **OK**.
5. To change the timeout period in Apache Tomcat for staying logged on to the Symantec Endpoint Protection Manager remote web console, on the server that runs Symantec Endpoint Protection Manager, open the following file in a text editor:

```
Program Files\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\conf.properties
```

6. Add the following line, if it is not present:

```
scm.web.timeout.minutes=timeout_value
```

The value `timeout_value` is the number of minutes of inactivity after which the console logs out. The maximum value is 60. A value of 0 has the same effect as not adding the line at all.

If this line is present, you can change the timeout value.

7. Save and close the file.
8. For your changes to take effect, open the Windows Services (`services.msc`) and restart the Symantec Endpoint Protection Manager service.
9. To change the timeout period in Internet Explorer for staying logged on to the Symantec Endpoint Protection Manager remote web console, follow the instructions in the Microsoft article, [How to change the default keep-alive timeout value in Internet Explorer](#), to change the registry key `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings`.
10. To change the timeout period in Mozilla Firefox for staying logged on to the Symantec Endpoint Protection Manager remote web console, in the address bar, enter the following:

```
about:config
```

11. Click to acknowledge the warning.

12. Search for the following line:

```
network.http.keep-alive.timeout
```

13. Change the value (in seconds) to the one that you want. The default is 115.

#### NOTE

Google Chrome does not have configurable settings for the network timeout period.

[Logging on to the Symantec Endpoint Protection Manager console](#)

## About domains

When you install a management server, the Symantec Endpoint Protection Manager console includes one domain, which is called Default. Domains are a logical separation of data that is separate from the Symantec Endpoint Protection Manager infrastructure. A domain is a structural container in the console that you use to organize a hierarchy of groups, clients, computers, and policies. You set up additional domains to manage your network resources.

---

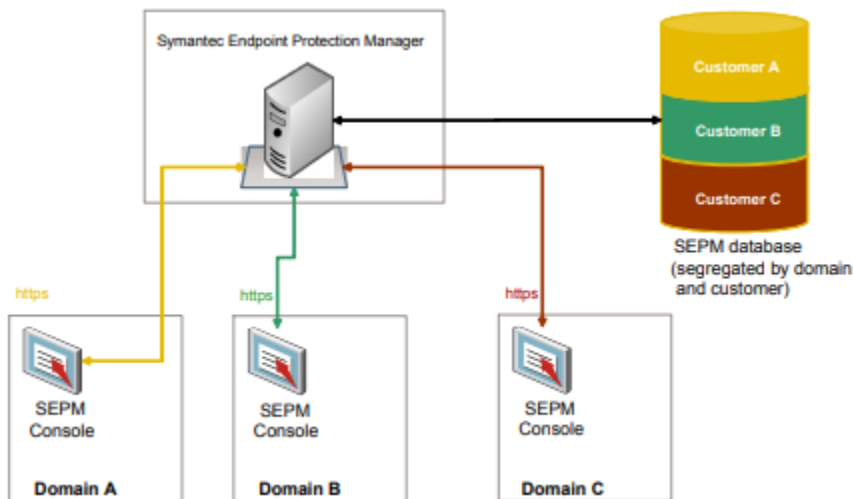
The primary purpose of domains is for managed service providers to build a single Symantec Endpoint Protection Manager infrastructure that services multiple customers.

#### NOTE

The domains in Symantec Endpoint Protection Manager are not equivalent to Windows domains or other network domains.

Each domain that you add shares the same management server and database, and it provides an additional instance of the console. All data in each domain is completely separate. This separation prevents administrators in one domain from viewing data in other domains. You can add an administrator account so that each domain has its own administrator. These administrators can view and manage only the contents of their own domain.

If your company is large, with sites in multiple regions, you may need to have a single view of management information. You can delegate administrative authority, physically separate security data, or have greater flexibility in how users, computers, and policies are organized. If you are a managed service provider (MSP), you may need to manage multiple independent companies, as well as Internet service providers. To meet these needs, you can create multiple domains. For example, you can create a separate domain for each country, region, or company.



When you add a domain, the domain is empty. You must set the domain to be the current domain. You then add administrators, groups, clients, computers, and policies to this domain.

You can copy policies from one domain to another. To copy policies between domains, you export the policy from the originating domain and you import the policy into the destination domain.

You can also move clients from one domain to another. To move clients between domains, the administrator of the old domain must delete the client from the client group. You then replace the Communication Settings file on the client with one from the new domain.

You can disable a domain if you no longer need it. Ensure that it is not set as the current domain when you attempt to disable it.

[Adding a domain](#)

[Switching to the current domain](#)

## Adding a domain

You create a domain to organize a hierarchy of groups, users, clients, and policies in your organization. For example, you may want to add domains to organize users by division.

---

## NOTE

You can use a domain ID for disaster recovery. If all the management servers in your organization fail, you need to rebuild the management server by using the same ID as the old server. You can get the old domain ID from the sylink.xml file on any client.

To add a domain

1. In the console, click **Admin**.
2. On the **Admin** page, click **Domains**.
3. Under Tasks, click **Add Domain**.
4. In the Add Domain dialog box, type a domain name, an optional company name, and optional contact information.
5. If you want to add a domain ID, click **Advanced** and then type the value in the text box.
6. Click **OK**.

### [About domains](#)

## Switching to the current domain

The default domain name is **Default**, and it is set as the current domain. When you add a new domain in the Symantec Endpoint Protection Manager console, the domain is empty. To add groups, clients, policies, and administrators to a new domain, you must first set it as the current domain. When a domain is designated as the current domain, the text **Current Domain** follows the domain name in the title. If you have many domains, you must scroll through the **Domains** list to display which domain is the current one.

If you logged on to the console as a system administrator, you can see all domains no matter which domain is the current one. However, you can only see the administrators and limited administrators that were created in the current domain. If you logged on to the console as either an administrator or a limited administrator, you only see the domain to which you have access.

If you remove the current domain, the management server logs you out. You can only remove a domain if it is not the current domain and not the only domain.

To switch to the current domain

1. In the console, click **Admin**.
2. On the **Admin** page, click **Domains**.
3. Under **Domains**, click the domain that you want to make the current domain.
4. Under **Tasks**, click **Administer Domain**.
5. In the Administer Domain dialog box, to confirm, click **Yes**.
6. Click **OK**.

### [About domains](#)

### [Adding a domain](#)



---

## Using Policies to Manage Security

---

Use policies to manage the security on your client computers

You use different types of security policies to manage your network security. Default policies are automatically created during the installation. You can use the default policies or you can customize policies to suit your specific environment.

### Performing the tasks that are common to all policies

Your security policies define how the protection technologies protect your computers from known and unknown threats.

You can manage your Symantec Endpoint Protection security policies in many ways. For example, you can create copies of the security policies and then customize the copies for your specific needs. You can lock and unlock certain settings so that users cannot change them on the client computer.

**Table 73: Tasks common to all policies**

Task	Description
Add a policy	<p>If you do not want to use one of the default policies, you can add a new policy. You can add shared policies or non-shared policies.</p> <p><b>Note:</b> If you add or edit shared policies in the <b>Policies</b> page, you must also assign the policies to a group or location. Otherwise those policies are not effective.</p> <p><a href="#">The types of security policies</a> <a href="#">About shared and non-shared policies</a> <a href="#">Adding a policy</a></p>
Lock and unlock policy settings	<p>You can allow or prevent client users from configuring some policy settings and client user interface settings.</p> <p><a href="#">Preventing users from disabling protection on client computers</a></p>
Edit a policy	<p>If you want to change the settings in an existing policy, you can edit it. You can increase or decrease the protection on your computers by modifying its security policies. You do not have to reassign a modified policy unless you change the group assignment.</p> <p><a href="#">Editing a policy</a></p>
Assign a policy	<p>To put a policy into use, you must assign it to one or more groups or locations.</p> <p><a href="#">Assigning a policy to a group or location</a></p>
Test a policy	<p>Symantec recommends that you always test a new policy before you use it in a production environment.</p>
Update the policies on clients	<p>Based on the available bandwidth, you can configure a client to use push mode or pull mode as its policy update method.</p> <p><a href="#">Updating policies and content on the client using push mode or pull mode</a></p>
Replace a policy	<p>You can replace a shared policy with another shared policy. You can replace the shared policy in either all locations or for one location.</p> <p><a href="#">Replacing a policy</a></p>
Copy and paste a policy	<p>Instead of adding a new policy, you may want to copy an existing policy to use as the basis for the new policy. You can copy and paste policies on either the <b>Policies</b> page or the <b>Policies</b> tab on the <b>Clients</b> page.</p> <p><b>Note:</b> You can also copy all the policies in a group and paste them into another group, from the <b>Policies</b> tab on the <b>Clients</b> page.</p> <p><a href="#">Copying and pasting a policy on the Clients page</a> <a href="#">Copying and pasting a policy on the Policies page</a></p>

Task	Description
Convert a shared policy to a non-shared policy	<p>You can copy the content of a shared policy and create a non-shared policy from that content.</p> <p><a href="#">About shared and non-shared policies</a></p> <p>A copy enables you to change the content of a shared policy in one location and not in all other locations. The copy overrides the existing non-shared policy.</p> <p>You can convert a shared policy to a non-shared policy if the policy no longer applies to all the groups or all the locations. When you finish the conversion, the converted policy with its new name appears under Location-specific Policies and Settings.</p> <p><a href="#">Converting a shared policy to a non-shared policy</a></p>
Export and import a policy	<p>You can export an existing policy if you want to use it at a different site or management server. You can then import the policy and apply it to a group or to a specific location.</p> <p><a href="#">Exporting and importing individual Endpoint Protection policies</a></p>
Withdraw a policy	<p>If you delete a policy, Symantec Endpoint Protection Manager removes the policy from the database. If you do not want to delete a policy, but you no longer want to use it, you can withdraw the policy instead.</p> <p>You can withdraw any type of policy except a <b>Virus and Spyware Protection policy</b> and a <b>LiveUpdate Settings policy</b>.</p> <p><a href="#">Unassigning a policy from a group or location</a></p>
Delete a policy	<p>If a policy is assigned to one or more groups and locations, you cannot delete it until you have unassigned it from all the groups and locations. You can also replace the policy with another policy</p>
Check that the client has the latest policy	<p>You can check whether the client has the latest policy. If not, you can manually update the policy on the client.</p> <p><a href="#">Using the policy serial number to check client-server communication</a></p> <p><a href="#">Updating client policies</a></p>

## The types of security policies

You use several different types of security policies to manage your network security. Most types of policies are automatically created during the installation. You can use the default policies or you can customize policies to suit your specific environment.

[Performing the tasks that are common to all policies](#)

**Table 74: Security policy types**

Policy type	Description
<b>Virus and Spyware Protection policy</b>	<p>The Virus and Spyware Protection policy provides the following protection:</p> <ul style="list-style-type: none"> <li>• Detects, removes, and repairs the side effects of virus and security risks by using signatures.</li> <li>• Detects the threats in the files that users try to download by using reputation data from Download Insight.</li> <li>• Detect the applications that exhibit suspicious behavior by using SONAR heuristics and reputation data.</li> </ul> <p>The <b>Virus and Spyware Protection policy</b> finds behavior anomalies through its SONAR technology.</p> <p><b>Note:</b> Download Insight and SONAR technology are available only on Windows clients.</p> <p><a href="#">Managing scans on client computers</a></p>
<b>Firewall policy</b>	<p><b>The Firewall policy provides the following protection:</b></p> <ul style="list-style-type: none"> <li>• Blocks the unauthorized users from accessing the computers and networks that connect to the Internet.</li> <li>• Detects the attacks by hackers.</li> <li>• Eliminates the unwanted sources of network traffic.</li> </ul> <p><b>Note:</b> Firewall policies can be applied only to Windows clients.</p> <p><a href="#">Managing firewall protection</a></p>
<b>Intrusion Prevention policy</b>	<p>The Intrusion Prevention policy automatically detects and blocks network attacks and attacks on browsers as well as protects applications from vulnerabilities.</p> <p><a href="#">Managing intrusion prevention</a></p>
<b>Application and Device Control</b>	<p>The Application and Device Control policy protects a system's resources from applications and manages the peripheral devices that can attach to computers.</p> <p><a href="#">Setting up application control</a></p> <p>Application Control policy can be applied only to Windows clients. The Device Control policy applies to Windows and Mac computers.</p>
<b>Host Integrity</b>	<p>The Host Integrity policy provides the ability to define, enforce, and restore the security of client computers to keep enterprise networks and data secure. You use this policy to verify that the clients that access your network run the antivirus software, patches, and other application criteria that you define.</p> <p><a href="#">Setting up Host Integrity</a></p>
<b>LiveUpdate policy</b>	<p>The LiveUpdate Content policy and the LiveUpdate Settings policy contain the settings that determine how and when client computers download content updates from LiveUpdate. You can define the computers that clients contact to check for updates and schedule when and how often client computers check for updates.</p> <p><a href="#">How to update content and definitions on the clients</a></p>
<b>Memory Exploit Mitigation</b>	<p>The Memory Exploit Mitigation policy stops vulnerability attacks on software using mitigation techniques such as DLL hijacking, heap spray mitigation, and Java exploit prevention.</p> <p><a href="#">Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy</a></p> <p>This policy type was added for 14.0.1. Version 14 added this functionality in the Intrusion Prevention policy under the name of Generic Exploit Mitigation.</p>

Policy type	Description
<b>Web and Cloud Access Protection</b>	<p>Web and Cloud Access Protection sends network traffic to a Symantec Web Security Service (WSS). The WSS solution protects users and organizations by categorizing applications and web sites, and then allowing or denying access to them based on policy.</p> <p>Web and Cloud Access Protection was renamed from Network Traffic Redirection in 14.3 RU2. Web and Cloud Access Protection</p> <p><a href="#">Configuring Web and Cloud Access Protection</a></p>
<b>Exceptions</b>	<p>The Exceptions policy provides the ability to exclude applications and processes from detection by the virus and spyware scans and by SONAR.</p> <p>You can also exclude applications from application control.</p> <p><a href="#">Managing exceptions in Symantec Endpoint Protection</a></p>

## Updating client policies

You can update the policies on the Symantec Endpoint Protection client computer if you do not think you have the latest. If the client does not receive the update, there might be a communication problem.

Check the policy serial number to check whether your managed client computers can communicate with the management server.

You can only manually update the policy on the client computer. If policy settings prevent you from opening the user interface or the notification area icon, you may not be able to manually update the policy.

No command exists in Symantec Endpoint Protection Manager to manually prompt the client to update policies. The client checks in for policy updates based on its update method of pull mode or push mode.

### To update the client policy on the client from the Windows taskbar:

1. In the Windows taskbar, in the notification area, right-click the Symantec Endpoint Protection icon.
2. Click **Update Policy**.

### To update the client policy from the client user interface:

1. In the client, click **Help > Troubleshooting**.
2. In the **Troubleshooting** dialog box, in the left column, click **Management**.
3. On the **Management** panel, under **Policy Profile**, click one of the following:
4. Click **Update** to update the policy directly from the management console.
5. Click **Import** to import the policy with one that was exported from the management console. Follow the prompt to select the policy file to import.

## Adding a policy

Symantec Endpoint Protection Manager comes with a default policy for each type of protection. If you need to customize a policy, you add one and edit it. You can create multiple versions of each type of policy.

Symantec recommends that you test all new policies before you use them in a production environment.

To add a new policy

- 
1. In the console, click **Policies**.
  2. On the **Policies** page, select a policy type, and then click the link to add a new policy.
  3. Modify the policy settings to increase or decrease protection.
  4. Click **OK** to save the policy.
  5. Optionally assign the new policy to a group.

You can assign a new policy to a group during or after policy creation. The new policy replaces the currently assigned policy of the same protection type.

[Assigning a policy to a group or location](#)

[Performing the tasks that are common to all policies](#)

## Editing a policy

You can edit shared and non-shared policies on the **Policies** tab on the **Clients** page as well as on the **Policies** page. Locations as well as groups can share the same policy. You must assign a shared policy after you edit it.

[Assigning a policy to a group or location](#)

1. **Option 1:** To edit a policy on the Policies page, in the console, click **Policies**.
2. On the **Policies** page, under **Policies**, click the policy type.
3. In the **policy type Policies** pane, click the specific policy that you want to edit
4. Under **Tasks**, click **Edit the Policy**.
5. In the **policy type Policy Overview** pane, edit the name and description of the policy, if necessary.
6. To edit the policy, click any of the **policy type Policy** pages for the policies.
7. **Option 2:** To edit a policy on the **Clients** page, in the console, click **Clients**.
8. On the **Clients** page, under **Clients**, select the group for which you want to edit a policy.
9. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.  
You must disable inheritance for this group. If you do not uncheck inheritance, you cannot edit a policy.
10. Under **Location-specific Policies and Settings**, scroll to find the name of the location whose policy you want to edit.
11. Locate the specific policy for the location that you want to edit.
12. To the right of the selected policy, click **Tasks**, and then click **Edit Policy**.
13. Do one of the following tasks:
  - To edit a non-shared policy, go to the next step.
  - To edit a shared policy, in the **Edit Policy** dialog box, click **Edit Shared** to edit the policy in all locations.
14. You can click a link for the type of policy that you want to edit.

## Finding a policy's default settings

If you have changed a policy's settings, you can return the policy to its default settings. You add a new policy of *<policy type>*, which includes the default settings automatically.

[Adding a policy](#)

---

## Copying and pasting a policy on the Policies page

You can copy and paste a policy on the **Policies** page. For example, you may want to edit the policy settings slightly to apply to another group.

1. To copy a policy in the **Policies** page, in the console, click **Policies**.
2. On the **Policies** page, under **Policies**, click the type of policy that you want to copy.
3. In the **policy type Policies** pane, click the specific policy that you want to copy.
4. On the **Policies** page, under **Tasks**, click **Copy the Policy**.
5. In the **Copy Policy** dialog box, check **Do not show this message again** if you no longer want to be notified about this process.

To redisplay the **Do not show this message again** check box, click **Admin > Administrators**, select your administrator account, and click **Reset Copy Policy Reminder**.

6. Click **OK**.
7. To paste a policy in the **Policies** page, in the console, click **Policies**.
8. On the **Policies** page, under **Policies**, click the type of policy that you want to paste.
9. In the **policy type Policies** pane, click the specific policy that you want to paste.
10. On the **Policies** page, under **Tasks**, click **Paste a Policy**.

### [Copying and pasting a policy on the Clients page](#)

## Copying and pasting a policy on the Clients page

You can copy and paste a policy instead of having to add a new policy. You can copy a shared or a non-shared policy on the **Clients** page.

### [Performing the tasks that are common to all policies](#)

1. To copy a policy in the **Clients** page, in the console, click **Clients**.
2. On the **Clients** page, under **Clients**, select the group for which you want to copy a policy.
3. On the **Policies** tab, under **Location-specific Policies and Settings**, scroll to find the name of the location from which you want to copy a policy.
4. Locate the specific policy for the location that you want to copy.
5. To the right of the policy, click **Tasks**, and then click **Copy**.
6. Click **OK**.
7. To paste a policy on the **Clients** page, in the console, click **Clients**.
8. On the **Clients** page, under **Clients**, select the group for which you want to paste a policy.
9. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.

You must disable inheritance for this group. If you do not uncheck inheritance, you cannot paste a policy.

10. Under **Location-specific Policies and Settings**, scroll to find the name of the location whose policy you want to paste.
11. Locate the specific policy for the location that you want to paste.
12. To the right of the policy, click **Tasks**, and then click **Paste**.
13. When you are prompted to overwrite the existing policy, click **Yes**.

## Assigning a policy to a group or location

You assign a policy to a client computer through a group. Every group has exactly one policy of each protection type that is assigned to it at all times. Typically, you create separate groups for the clients that run different platforms. If you put the clients that run different platforms into the same group, each client platform ignores any settings that do not apply to it.







Unassigned policies are not downloaded to the client computers in groups and locations. If you do not assign the policy when you add the policy, you can assign it to groups and locations later. You can also reassign a policy to a different group or location.

### Policies are assigned to computer groups as follows:

- At initial installation, the Symantec default security policies are assigned to the **My Company** parent group.
- The security policies in the **My Company** parent group are automatically assigned to each newly created child group. Newly created child groups inherit from **My Company** by default.  
New groups always inherit from their immediate parent group. If you create a hierarchy of child groups, each one inherits from its immediate parent, not from the top-level parent.
- You replace a policy in a group by assigning another policy of the same type. You can replace a policy that is assigned to the **My Company** parent group or to any child group.

The icons display the following information:

**Table 75: Policy icons**

Icon	Description
	A group without a policy that is assigned to it.
	A group with a policy assigned to it. The text is bold.
	A location without a policy that is assigned to it.
	A location with a policy assigned to it. The text is bold.
	A location that inherits from a parent group and has no policy that is assigned to it.
	A location that inherits from a parent group and has a policy that is assigned to it

To assign a policy to a group or location

1. In the console, click **Policies** > policy type.
2. On the **Policies** page, select a policy, and then click **Assign the policy**.
3. In the **Assign policy** dialog box, select the groups or locations, and then click **Assign**.
4. Click **OK** to confirm.

### Unassigning a policy from a group or location

---

## Replacing a policy

You may want to replace one shared policy with another shared policy. You can replace the shared policy in either all locations or for individual locations.

When you replace a policy for all locations, the management server replaces the policy only for the locations that have it. For example, suppose the Sales group uses the Sales policy for three of its four locations. If you replace the Sales policy with the Marketing policy, only those three locations receive the Marketing policy.

You may want a group of clients to use the same settings no matter what location they are in. In this case, you can replace a non-shared policy with a shared policy. You replace a non-shared policy with a shared policy for each location individually.

### Performing the tasks that are common to all policies

1. To replace a shared policy for all locations, in the console, click **Policies**.
2. On the **Policies** page, under **Policies**, click the type of policy that you want to replace.
3. In the **policy type Policies** pane, click the policy.
4. In the **Policies** page, under **Tasks**, click **Replace the Policy**.
5. In the **Replace policy type Policy** dialog box, in the **New policy type Policy** list box, select the shared policy that replaces the old one.
6. Select the groups and locations for which you want to replace the existing policy.
7. Click **Replace**.
8. When you are prompted to confirm the replacement of the policy for the groups and locations, click **Yes**.
9. To replace a shared policy or non-shared policy for one location, in the console, click **Clients**.
10. In the **Clients** page, under **Clients**, select the group for which you want to replace a policy.
11. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.  
You must disable inheritance for this group. If you do not uncheck inheritance, you cannot replace a policy.
12. Under **Location-specific Policies and Settings**, scroll to find the location that contains the policy.
13. Next to the policy that you want to replace, click **Tasks**, and then click **Replace Policy**.
14. In the **Replace Policy** dialog box, in the **New policy** list box, select the replacement policy.
15. Click **OK**.

## Exporting and importing individual Endpoint Protection policies

You can export and import policies rather than recreating the policies. All the settings that are associated with the policy are automatically exported.

### You may need to export a policy for the following reasons:

- You update the management server from an older release to a newer release. You want to update the new management server with the policies that you previously customized.
- You want to export a policy for use at a different site.

You export and import each policy one at a time. Once you export a file, you import it and apply it to a group or only to a location. You can export a shared or non-shared policy for a specific location in the **Clients** page.



---

## Performing the tasks that are common to all policies

1. To export a single policy from the **Policies** page, in the console, click **Policies**.
2. On the **Policies** page, under **Policies**, click the type of policy that you want to export.
3. In the **policy type Policies** pane, click the specific policy that you want to export.
4. In the **Policies** page, under **Tasks**, click **Export the Policy**.
5. In the **Export Policy** dialog box, locate the folder where you want to export the policy file to, and then click **Export**.
6. To export a shared or non-shared policy from the **Clients** page, in the console, click **Clients**.
7. Under **Clients**, select the group for which you want to export a policy.
8. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.  
You must disable inheritance for this group. If you do not uncheck inheritance, you cannot export a policy.
9. Under **Location-specific Policies and Settings**, scroll to find the name of the location whose policy you want to export.
10. Locate the specific policy for the location that you want to export.
11. To the right of the policy, click **Tasks**, and then click **Export Policy**.
12. In the **Export Policy** dialog box, browse to the folder into which you want to export the policy.
13. In the **Export Policy** dialog box, click **Export**.
14. To import a single policy, in the console, click **Policies**.
15. On the **Policies** page, under **Policies**, click the type of policy that you want to import.
16. In the **policy type Policies** pane, click the policy that you want to import.
17. On the **Policies** page, under **Tasks**, click **Import a policy type Policy**.
18. In the **Import Policy** dialog box, browse to the policy file that you want to import, and then click **Import**.

## About shared and non-shared policies

Policies are either shared or non-shared. A policy is shared if you apply it to more than one group or location. If you create shared policies, you can easily edit and replace a policy in all groups and locations that use it. You can apply shared policies at the My Company group level or a lower group level and subgroups can inherit policies. You can have multiple shared policies.

If you need a specialized policy for a particular group or location, you create a policy that is unique. You assign this unique, non-shared policy to one specific group or location. You can only have one policy of each policy type per location.

### For example, here are some possible scenarios:

- A group of users in Finance needs to connect to an enterprise network by using different locations when at the office and for home. You may need to apply a different Firewall policy with its own set of rules and settings to each location for that one group.
- You have remote users who typically use DSL and ISDN, for which they may need a VPN connection. You have other remote users who want to dial up when they connect to the enterprise network. However, the sales and marketing groups also want to use wireless connections. Each of these groups may need its own Firewall policy for the locations from which they connect to the enterprise network.
- You want to implement a restrictive policy regarding the installation of non-certified applications on most employee workstations to protect the enterprise network from attacks. Your IT group may require access to additional applications. Therefore, the IT group may need a less restrictive security policy than typical employees. In this case, you can create a different Firewall policy for the IT group.

---

You typically add any policy that groups and locations share in the **Policies** page on the **Policies** tab. However, you add any policy that is not shared between groups and that applies only to a specific location in the **Clients** page. If you decide to add a policy in the **Clients** page, you can add a new policy by using any of the following methods:

- Add a new policy.  
[Adding a policy](#)
- Copy an existing policy to base the new policy on.  
[Copying and pasting a policy on the Policies page](#)  
[Copying and pasting a policy on the Clients page](#)
- Import a policy that was previously exported from another site.  
[Exporting and importing individual Endpoint Protection policies](#)

[Performing the tasks that are common to all policies](#)

[Converting a shared policy to a non-shared policy](#)

## Converting a shared policy to a non-shared policy

You can copy the content of a shared policy and create a non-shared policy from that content. A copy enables you to change the content of a shared policy in one location and not in all other locations. The copy overrides the existing shared policy.

When you finish the conversion, the converted policy with its new name appears under **Location-specific Policies and Settings**. However, the non-shared policy does not appear in the **Policies** page for the policy type unless you copy it from the **Clients** page > **Policies** tab to the **Policies** page.

[About shared and non-shared policies](#)

[Copying and pasting a policy on the Clients page](#)

[Copying and pasting a policy on the Policies page](#)

To convert a shared policy to a non-shared policy

1. In the console, click **Clients**.
2. In the **Clients** page, under **Clients**, select the group for which you want to convert a policy.
3. In the pane that is associated with the group that you selected in the previous step, click **Policies**.
4. On the **Policies** tab, uncheck **Inherit policies and settings from parent group group\_name**.  
You must disable inheritance for this group. If you do not uncheck inheritance, you cannot replace a policy.
5. Under **Location-specific Policies and Settings**, scroll to find the name of the location and the specific policy that you want to convert.
6. Beside the specific policy, click **Tasks**, and then click **Convert to Non-shared Policy**.
7. In the **Overview** dialog box, edit the name and description of the policy.
8. Modify the other policy settings as desired.
9. Click **OK**.

[Performing the tasks that are common to all policies](#)

## Unassigning a policy from a group or location

You may want to unassign a policy from a group or a location if you want to delete the policy permanently or save the policy to use for a later time.

---

For example, a specific group may have experienced problems after you introduced a new policy. If you want the policy to remain in the database, you can withdraw the policy instead of deleting it. If you withdraw a policy, it is automatically withdrawn from the groups and locations that you assigned it to. The number of locations that a policy is used for appears on the **policy type Policies** pane on the **Policies** page.

#### NOTE

You must withdraw a policy or replace a policy from all groups and locations before you can delete it.

**You can withdraw all policies in the Policies page from a location or group except for the following policies:**

- **Virus and Spyware Protection**
- **LiveUpdate Settings**

You can only replace them with another **Virus and Spyware Protection** policy or **LiveUpdate** policy.

[Replacing a policy](#)

[Assigning a policy to a group or location](#)

1. To unassign a shared policy in the **Policies** page, in the console, click **Policies**.
2. On the **Policies** page, under **Policies**, click the type of policy that you want to withdraw.
3. In the **policy type Policies** pane, click the specific policy that you want to withdraw.
4. On the **Policies** page, under **Tasks**, click **Withdraw the Policy**.
5. In the **Withdraw Policy** dialog box, check the groups and locations from which you want to withdraw the policy.
6. Click **Withdraw**.
7. When you are prompted to confirm the withdrawal of the policy from the groups and locations, click **Yes**.
8. To unassign a shared or non-shared policy in the **Clients** page, in the console, click **Clients**.
9. On the **Clients** page, under **Clients**, select the group for which you want to withdraw a policy.
10. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.  
You must disable inheritance for this group. If you do not uncheck inheritance, you cannot withdraw a policy.
11. Under **Location-specific Policies and Settings**, scroll to find the name of the location for which you want to withdraw a policy.
12. Locate the policy for the location that you want to withdraw.
13. Click **Tasks**, and then click **Withdraw Policy**.
14. In the **Withdraw Policy** dialog box, click **Yes**.

[Performing the tasks that are common to all policies](#)

## Preventing users from disabling protection on client computers

As the Symantec Endpoint Protection Manager administrator, you prevent users from disabling protection on the client computer by setting the user control level or by locking the policy options. For example, the firewall policy uses a control level, whereas Virus and Spyware Protection policy uses a lock.

Symantec recommends that you prevent users from disabling protection at all times.

- [What are the user control levels?](#)
- [Changing the user control level](#)
- [Locking and unlocking policy settings](#)
- [Preventing users from disabling specific protection technologies](#)
- [Updating the client policy from Symantec Endpoint Protection Manager](#)

### What are the user control levels?

You use the user control levels to give the client user control of specific features. The user control level also determines whether the client user interface can be completely invisible, display a partial set of features, or display in full.

**Table 76: User control levels**

User control level	Description
Server control	Gives the users the least control over the client. With server control, the user can make changes to unlocked settings, but they are overwritten at the next heartbeat.
Client control	Gives the users the most control over the client. Client control allows users to configure the settings. Client-modified settings take precedence over server settings. They are not overwritten when the new policy is applied, unless the setting has been locked in the new policy. Client control is useful for employees who work in a remote location or a home location. <b>Note:</b> The user must be in a Windows administrators group to change any of the settings in <b>Client control</b> mode or <b>Mixed control</b> mode.
Mixed control	Gives the user a mixture of control over the client. You determine which options you let users configure by setting the option to <b>Server control</b> or to <b>Client control</b> . For those items that are under client control, the user retains control over the setting. For those items that are under server control, you retain control over the setting.

For the Windows client, you can configure all the options. For the Mac client, only the notification area icon and some IPS options are available in server control and client control.

Clients that run in **Client control** or **Mixed control** switch to **Server control** when the server applies a Quarantine policy.

### [Preventing and allowing users to change the client's user interface](#)

#### Changing the user control level

Some managed settings have dependencies. For example, users may have permission to configure firewall rules, but cannot access the client user interface. Because users do not have access to the **Configure Firewall Rules** dialog box, they cannot create rules.

1. In the console, click **Clients**.
2. Under **View Clients**, select the group, and click the **Policies** tab.
3. Under **Location-specific Policies and Settings**, under the location you want to modify, expand **Location-specific Settings**.
4. Next to **Client User Interface Control Settings**, click **Tasks > Edit Settings**.
5. In the **Client User Interface Control Settings** dialog box, do one of the following options:
  - Click **Server control**, and then click **Customize**.  
Configure any of the settings, and then click **OK**.
  - Click **Client control**.
  - Click **Mixed control**, and then click **Customize**.  
Configure any of the settings, and then click **OK**.
6. Click **OK**.

### [Configuring firewall settings for mixed control](#)

---

## Locking and unlocking policy settings

You can lock and unlock some policy settings. Users cannot change locked settings. A padlock icon appears next to a lockable setting. You can lock and unlock Virus and Spyware Protection settings, Tamper Protection settings, Submissions settings, and intrusion prevention settings.

### Preventing users from disabling specific protection technologies

If you set the client to **Mixed control** or **Server control** but do not lock the options, then the user can change the settings. These changes remain in place until the next heartbeat with Symantec Endpoint Protection Manager. Locking the policy options in the various policies ensures that the user cannot make any changes to the settings, even in **Client control**.

#### NOTE

Windows users who are not the Administrators group cannot change settings in the Symantec Endpoint Protection client user interface, regardless of the **Location-specific Settings** configuration. Windows 10 Administrators can still disable the product through the notification area icon even after you set these options. However, they cannot disable the individual protection technologies through the client user interface.

#### NOTE

If you do not want to change policies for all groups, disable policy inheritance on the group on which you want to make changes. If you edit a shared policy, the edited policy applies to every group to which the shared policy applies, even with policy inheritance disabled.

### To prevent users from disabling the firewall or Application and Device Control

1. In the console, click **Clients**.
2. Click the client group that you want to restrict, and then click the **Policies** tab.
3. Expand **Location-specific Settings**.
4. Next to **Client User Interface Control Settings**, click **Tasks > Edit Settings**.
5. Click **Server control** or **Mixed control**, and then click **Customize**.
6. On the **Client User Interface Settings** dialog box (server control) or pane (mixed control), uncheck **Allow the following users to enable and disable the firewall** and **Allow user to enable and disable the application device control**.
7. Click **OK**, and then click **OK** again.

### To prevent users from disabling intrusion prevention

1. In the console, click **Clients**.
2. Click the client group that you want to restrict, and then click the policy **Policies** tab.
3. Expand **Location-specific Policies**.
4. Next to **Intrusion Prevention policy**, click **Tasks > Edit Policy**.
5. Click **Intrusion Prevention**, and then click the locks next to **Enable Network Intrusion Prevention** and **Enable Browser Intrusion Prevention** to lock these features.
6. Click **OK**.

### To prevent users from disabling Virus and Spyware Protection

1. In the console, click **Clients**.
2. Click the client group that you want to restrict, and then click the **Policies** tab.
3. Expand **Location-specific Policies**.
4. Next to **Virus and Spyware Protection policy**, click **Tasks > Edit Policy**.
5. Under **Windows Settings**, lock the following features:

- 
- Click **Auto-Protect**, and then click the lock next to **Enable Auto-Protect**.
  - Click **Download Protection**, and then click the lock next to **Enable Download Insight to detect potential risks downloaded files based on file reputation**.
  - Click **SONAR**, and then click the lock next to **Enable SONAR**.
  - Click **Early Launch Anti-Malware Driver**, and then click the lock next to **Enable Symantec early launch anti-malware**.
  - Click **Microsoft Outlook Auto-Protect**, and then click the lock next to **Enable Microsoft Outlook Auto-Protect**.
  - For versions earlier than 14.2 RU1, click **Internet Email Auto-Protect**, and then click the lock next to **Enable Internet Email Auto-Protect**.
  - For versions earlier than 14.2 RU1, click **Lotus Notes Auto-Protect**, and then click the lock next to **Enable Lotus Notes Auto-Protect**.
  - Click **Global Scan Options**, and then click the locks next to **Enable Insight for** and **Enable Bloodhound heuristic virus detection**.
6. Click **OK**.

### To prevent users from disabling Memory Exploit Mitigation (14.1 or later)

In version 14, **Memory Exploit Mitigation** appeared in the Intrusion Prevention policy and was called **Generic Exploit Mitigation**.

1. In the console, click **Clients**.
2. Click the client group that you want to restrict, and then click the policy **Policies** tab.
3. Expand **Location-specific Settings**.
4. Next to **Memory Exploit Mitigation**, click **Tasks > Edit Policy**.
5. Click **Memory Exploit Mitigation**, and then click the lock next to **Enable Memory Exploit Mitigation**.
6. Click **OK**.

### Updating the client policy from Symantec Endpoint Protection Manager

After you make these changes, the clients in the group receive the updated policies depending on the group's communication settings. If the group is in push mode, Symantec Endpoint Protection Manager prompts the client to check in with a few seconds. If the group is in pull mode, the client checks in on the next scheduled heartbeat.

If you want them to have it sooner than the next heartbeat, you can prompt the client to check in and update its policy. You can also update the policy from the Symantec Endpoint Protection client.

#### Updating client policies

Once the client updates the policy, **Disable Symantec Endpoint Protection** is grayed out when you right-click the Symantec Endpoint Protection notification area icon.

## Monitoring the applications and services that run on client computers

The Windows client monitors and collects information about the applications and the services that run on each computer. You can configure the client to collect the information in a list and send the list to the management server. The list of applications and their characteristics is called learned applications.

You can use this information to find out what applications your users run. You can also use the information when you need information about applications in the following areas:

- Firewall policies
- Application and Device Control policies
- SONAR technology
- Host Integrity policies
- Network application monitoring
- File fingerprint lists

---

## NOTE

The Mac and Linux clients do not monitor the applications and the services that run on those computers.

You can perform several tasks to set up and use learned applications.

**Table 77: Steps to monitor the applications**

Steps	Description
Enable learned applications	Configure the management server to collect information about the applications that the client computers run. <a href="#">Collecting information about the applications that the client computers run</a>
Search for applications	You can use a query tool to search for the list of applications that the client computers run. You can search on application-based criteria or computer-based criteria. For example, you can find out the version of Internet Explorer that each client computer uses. <a href="#">Searching for information about the applications that the computers run</a> You can save the results of an application search for review.

## NOTE

In some countries, it may not be permissible under local law to use the learned applications tool under certain circumstances, such as to gain application use information from a laptop when the employee logs on to your office network from home using a company laptop. Before your use of this tool, please confirm that use is permitted for your purposes in your jurisdiction. If it is not permitted, please follow instructions for disabling the tool.

## Enabling application learning

You can enable learned applications for a group or a location, which collects information about the applications that the client computers run. The clients then keep track of every application that runs and send that data to the management server.

Because learned application data is forwarded to the management server by individual Symantec Endpoint Protection clients, the Symantec Endpoint Protection Manager bears the majority of the processing duties in ensuring this data is processed and stored in the SQL Server database. The more systems that forward learned application data, and the larger variety of applications run in an environment, the more information has to be temporarily stored, and then processed by the Symantec Endpoint Protection Manager. This can generate higher wait times on other SEP client data such as operational state data, or security log data. In very busy environments, this can generate CPU or memory issues for already under-resourced SEPMS.

## NOTE

The Mac and Linux clients do not support learned applications.

### To enable application learning for a group:

1. In the console, click **Clients**, select a group, and then click **Policies**.
2. On the **Policies** tab, click **Communications Settings**.
3. In the **Communications Settings** dialog box, check **Learn applications that run on the client computers**, and then click **OK**.

### To enable application learning for a location:

1. In the console, click **Clients**, select a group, and then click **Policies**.
2. On the **Policies** tab, select the location, and then expand **Location-specific Settings**.
3. To the right of **Communications Settings**, click **Tasks**, and then uncheck **Use Group Communications Settings** and click **Edit Settings**.



- 
4. In the **Communications Settings for location name** dialog box, check **Learn applications that run on the client computers**, and then click **OK**

**To enable application learning for the site:**

1. In the console, click **Admin > Servers**, and then click **Edit Site Properties**.
2. On the **General** tab, check **Keep track of every application that the clients run**.
3. To reduce the size of the default database, check **Delete learned application data after x days**. If you have trouble updating the management server database, Symantec recommends you enter 7.
4. Click **OK**.

You can set up a notification to be sent to your email address when each client in a group or location runs an application.

[Setting up administrator notifications](#)

[Monitoring the applications and services that run on client computers](#)

[Performing the tasks that are common to all policies](#)

## Searching for information about the learned applications that the computers run

After the management server receives the list of learned applications from the clients, you can run queries to find out details about the applications. For example, you can find all the client computers that use an unauthorized application. You can then create a firewall rule to block the application on the client computer. Or you may want to upgrade all the client computers to use the most current version of Microsoft Word. You can use the **Search for Applications** task from any type of policy.

### NOTE

The Mac client does not monitor the applications and the services that run on Mac computers.

You can search for an application in the following ways:

- By application.  
You can limit the search to specific applications or application details such as its name, file fingerprint, path, size, version, or last modified time.
- By client or client computer.  
You can search for the applications that either a specific user runs or a specific computer runs. For example, you can search on the computer's IP address.

You can also search for application names to add to a firewall rule, directly within the Firewall policy.

[Defining information about applications](#)

### NOTE

The information in the **Search** box is not collected until you enable the feature that keeps track of all the applications that clients run. You can go to the **Clients** page, **Communications Settings** dialog box for each group or location to enable this feature.

**To search for information about the applications that the computers run:**

1. In the console, click **Policies**.
2. On the **Policies** page, under **Tasks**, click **Search for Applications**.
3. In the **Search for Applications** dialog box, to the right of the **Search for applications in** field, click **Browse**.
4. In the **Select Group or Location** dialog box, select a group of clients for which you want to view the applications, and then click **OK**.

You can specify only one group at a time.



- 
5. Make sure that **Search subgroups** is checked.
  6. Do one of the following actions:
    - To search by user or computer information, click **Based on client/computer information**.
    - To search by application, click **Based on applications**.
  7. Click the empty cell under **Search Field**, and then select the search criterion from the list.

The Search Field cell displays the criteria for the option that you selected. For details about these criteria, click **Help**.
  8. Click the empty cell under Comparison Operator, and then select one of the operators.
  9. Click the empty cell under Value, and then select or type a value.

The Value cell may provide a format or a value from the drop-down list, depending on the criterion you selected in the Search Field cell.
  10. To add an additional search criterion, click the second row, and then enter information in the Search Field, Comparison Operator, and Value cells.

If you enter more than one row of search criteria, the query tries to match all conditions.
  11. Click **Search**.
  12. In the Query Results table, do any of the following tasks:
    - Click the scroll arrows to view additional rows and columns.
    - Click **Previous** and **Next** to see additional screens of information.
    - Select a row, and then click **View Details** to see additional information about the application.

The results are not saved unless you export them to a file.
  13. To remove the query results, click **Clear All**.
  14. Click **Close**.

[Monitoring the applications and services that run on client computers](#)

[Performing the tasks that are common to all policies](#)

## Managing firewall protection

The firewall allows the incoming network traffic and outgoing network traffic that you specify in the firewall policy. The Symantec Endpoint Protection firewall policy contains rules and protection settings, most of which you can enable or disable and configure.

**Table 78: Optional tasks to manage firewall protection**

Task	Description
Read about firewall protection	Before you configure your firewall protection, you should familiarize yourself with the firewall. <a href="#">How a firewall works</a> <a href="#">About the Symantec Endpoint Protection firewall</a>
Create a firewall policy	Symantec Endpoint Protection installs with a default firewall policy. You can modify the default policy or create new ones. You must create a policy first before you configure firewall rules and firewall protection settings for that policy. <a href="#">Creating a firewall policy</a>

Task	Description
Create and customize firewall rules	<p>Firewall rules are the policy components that control how the firewall protects client computers from malicious attacks.</p> <p>The default firewall policy contains default firewall rules. And when you create a new policy, Symantec Endpoint Protection provides default firewall rules. However, you can modify the default rules or create new ones.</p> <p><a href="#">Adding a new firewall rule</a></p> <p><a href="#">Customizing firewall rules</a></p>
Enable firewall protection settings	<p>After the firewall has completed certain operations, control is passed to a number of components. Each component is designed to perform a different type of packet analysis.</p> <p><a href="#">Enabling communications for network services instead of adding a rule</a></p> <p><a href="#">Automatically blocking connections to an attacking computer</a></p> <p><a href="#">Preventing outside stealth attacks on computers</a></p> <p><a href="#">Disabling the Windows Firewall</a></p> <p><a href="#">Blocking a remote computer by configuring peer-to-peer authentication</a></p>
Monitor firewall protection	<p>Regularly monitor the firewall protection status on your computers.</p> <p><a href="#">Monitoring endpoint protection</a></p>

[Running commands on client computers from the console](#)

[Configuring firewall settings for mixed control](#)

## How a firewall works

A firewall does all of the following tasks:

- Prevents any unauthorized users from accessing the computers and networks in your organization that connect to the Internet
- Monitors the communication between your computers and other computers on the Internet
- Creates a shield that allows or blocks attempts to access the information on your computer
- Warns you of connection attempts from other computers
- Warns you of connection attempts by the applications on your computer that connect to other computers

The firewall reviews the packets of data that travel across the Internet. A packet is a discrete unit of data that is part of the information flow between two computers. Packets are reassembled at their destination to appear as an unbroken data stream.

Packets include the following information about the data:

- The originating computer
- The intended recipient or recipients
- How the packet data is processed
- Ports that receive the packets

Ports are the channels that divide the stream of data that comes from the Internet. Applications that run on a computer listen to the ports. The applications accept the data that is sent to the ports.

Network attacks exploit weaknesses in vulnerable applications. Attackers use these weaknesses to send the packets that contain malicious programming code to ports. When vulnerable applications listen to the ports, the malicious code lets the attackers gain access to the computer.

## About the Symantec Endpoint Protection firewall

The Symantec Endpoint Protection firewall uses firewall policies and rules to allow or block network traffic. The Symantec Endpoint Protection includes a default Firewall policy with default firewall rules and firewall settings for the office environment. The office environment is normally under the protection of corporate firewalls, boundary packet filters, or

---

antivirus servers. Therefore, it is normally more secure than most home environments, where limited boundary protection is available.

Firewall rules control how the client protects the client computer from malicious inbound traffic and malicious outbound traffic. The firewall automatically checks all the inbound and the outbound packets against these rules. The firewall then allows or blocks the packets based on the information that is specified in rules. When a computer tries to connect to another computer, the firewall compares the type of connection with its list of firewall rules. The firewall also uses stateful inspection of all network traffic.

When you install the console for the first time, it adds a default Firewall policy to each group automatically.

Every time you add a new location, the console copies a Firewall policy to the default location automatically.

You determine the level of interaction that you want users to have with the client by permitting or blocking their ability to configure firewall rules and firewall settings. Users can interact with the client only when it notifies them of new network connections and possible problems. Or they can have full access to the user interface.

You can install the client with default firewall settings. In most cases you do not have to change the settings. However, if you have a detailed understanding of networks, you can make many changes in the client firewall to fine-tune the client computer's protection.

As of version 14.2, the Mac client offers a firewall for the managed client only. The user can only enable or disable the firewall if the administrator has allowed client control. Since it operates on a different network layer than the Mac's operating system firewall, they can both be enabled and run in parallel.

[About firewall settings for the Mac client](#)

[Managing firewall protection](#)

[How a firewall works](#)

[How the firewall uses stateful inspection](#)

[The types of security policies](#)

## About firewall settings for the Mac client

The firewall settings that are included in the Symantec Endpoint Protection client for Mac are as follows:

- Firewall smart rules
- Custom firewall rules

These settings are only configurable by the Symantec Endpoint Protection Manager administrator. The firewall is only available to managed clients.

The firewall is included with the Symantec Endpoint Protection client for Mac as of version 14.2.

**Table 79: Firewall settings**

Setting type	Description
Firewall smart rules	<p>Firewall smart rules provide protection to prevent common types of attack. They also allow traffic on specific protocols when the Mac makes the initial request on that protocol.</p> <p>Protection settings include:</p> <ul style="list-style-type: none"><li>• Portscan detection</li><li>• Denial of service detection</li><li>• Anti-MAC spoofing</li><li>• Automatically block an attacker's IP address</li></ul> <p>Traffic protocols include:</p> <ul style="list-style-type: none"><li>• Smart DHCP</li><li>• Smart DNS</li></ul> <p>The Symantec Endpoint Protection firewall for Mac does not integrate with the operating system's built-in firewall. Instead, it runs in parallel. The operating system firewall inspects at the Application layer, while the Symantec Endpoint Protection firewall inspects at lower levels (Network and Transport).</p> <p>The Symantec Endpoint Protection firewall for Mac does not offer peer-to-peer blocking rules, though you could create these in part through custom firewall rules.</p>
Custom firewall rules	<p>Custom firewall rules allow the administrator to create the rules that involve various attributes of the network traffic.</p>

## Managing firewall protection

### Creating a firewall policy

The Symantec Endpoint Protection includes a default Firewall policy with default firewall rules and default firewall settings for the office environment. The office environment is normally under the protection of corporate firewalls, boundary packet filters, or antivirus servers. Therefore, it is normally more secure than most home environments, where limited boundary protection is available.

When you install the console for the first time, it adds a default Firewall policy to each group automatically.

#### NOTE

Changing the name of the default Firewall policy may result in an upgrade not updating the policy. The same applies to the default rules within the default Firewall policy.

Every time you add a new location, the console copies a Firewall policy to the default location automatically. If the default protection is not appropriate, you can customize the Firewall policy for each location, such as for a home site or customer site. If you do not want the default Firewall policy, you can edit it or replace it with another shared policy.

[How to create a firewall policy](#) describes the tasks that you can perform to configure a new firewall policy. You must add a firewall policy first, but thereafter, the remaining tasks are optional and you can complete them in any order.

**Table 80: How to create a firewall policy**

Task	Description
Add new firewall rules	<p>Firewall rules are the policy components that control how the firewall protects client computers from malicious incoming traffic and applications. The firewall automatically checks all incoming packets and outgoing packets against these rules. It allows or blocks the packets based on the information that is specified in rules. You can modify the default rules, create new rules, or disable the default rules.</p> <p>When you create a new Firewall policy, Symantec Endpoint Protection provides default firewall rules that are enabled by default.</p> <p><a href="#">Adding a new firewall rule</a></p>
Enable and customize notifications to users that access to an application is blocked	<p>You can send users a notification that an application that they want to access is blocked. These settings are disabled by default.</p> <p><a href="#">Notifying the users that access to an application is blocked</a></p>
Enable automatic firewall rules	<p>You can enable the options that automatically permit communication between certain network services. These options eliminate the need to create the rules that explicitly allow those services. You can also enable traffic settings to detect and block the traffic that communicates through NetBIOS and token rings.</p> <p>Only the traffic protocols are enabled by default.</p> <p><a href="#">Enabling communications for network services instead of adding a rule</a></p> <p>If the Symantec Endpoint Protection client detects a network attack, it can automatically block the connection to ensure that the client computer is safe. The client activates an Active Response, which automatically blocks all communication to and from the attacking computer for a set period of time. The IP address of the attacking computer is blocked for a single location.</p> <p>This option is disabled by default.</p> <p><a href="#">Automatically blocking connections to an attacking computer</a></p>
Configure protection and stealth settings	<p>You can enable settings to detect and log potential attacks on the client and block spoofing attempts. You can enable the settings that prevent outside attacks from detecting information about your clients.</p> <p><a href="#">Preventing outside stealth attacks on computers</a></p> <p>All of the protection options and stealth options are disabled by default.</p>
Integrate the Symantec Endpoint Protection firewall with the Windows firewall	<p>You can specify the conditions in which Symantec Endpoint Protection disables the Windows firewall. When Symantec Endpoint Protection is uninstalled, Symantec Endpoint Protection restores the Windows firewall setting to the state it was in before Symantec Endpoint Protection was installed.</p> <p>The default setting is to disable the Windows firewall once only and to disable the Windows firewall disabled message.</p> <p><a href="#">Disabling the Windows Firewall</a></p>
Configure peer-to-peer authentication	<p>You can use peer-to-peer authentication to allow a remote client computer (peer) to connect to another client computer (authenticator) within the same corporate network. The authenticator temporarily blocks inbound TCP and UDP traffic from the remote computer until the remote computer passes the Host Integrity check.</p> <p>This option is disabled by default.</p> <p><a href="#">Blocking a remote computer by configuring peer-to-peer authentication</a></p>

**When you enable firewall protection, the policy allows all inbound IP-based network traffic and all outbound IP-based network traffic, with the following exceptions:**

- The default firewall protection blocks inbound and outbound IPv6 traffic with all remote systems.

---

## NOTE

IPv6 is a network layer protocol that is used on the Internet. If you install the client on the computers that run Microsoft Vista, the **Rules** list includes several default rules that block the Ethernet protocol type of IPv6. If you remove the default rules, you must create a rule that blocks IPv6.

- The default firewall protection restricts the inbound connections for a few protocols that are often used in attacks (for example, Windows file sharing).

Internal network connections are allowed and external networks are blocked.

[Managing firewall protection](#)

[Best practices for Firewall policy settings for remote clients](#)

## Managing firewall rules

Firewall rules control how the firewall protects computers from malicious incoming traffic and applications. The firewall checks all incoming packets and outgoing packets against the rules that you enable. It allows or blocks the packets based on the conditions that you specify in the firewall rule.

The Symantec Endpoint Protection client includes default firewall rules to protect your computer. However, you can modify the firewall rules for additional protection if your administrator permits it, or if your client is unmanaged.

Symantec Endpoint Protection installs with a default firewall policy that contains default rules. When you create a new firewall policy, Symantec Endpoint Protection provides default firewall rules. You can modify any of the default rules or create new firewall rules if your administrator permits it, or if your client is unmanaged.

You must have at least one rule in a policy. But you can have as many rules as you need. You can enable or disable rules as needed. For example, you might want to disable a rule to perform troubleshooting and enable it when you are done.

[Managing firewall rules](#) describes what you need to know to manage firewall rules.

**Table 81: Managing firewall rules**

Task	Description
Learn how firewall rules work and what makes up a firewall rule	<p>Before you modify the firewall rules, you should understand the following information about how firewall rules work:</p> <ul style="list-style-type: none"><li>How to order rules to ensure that the most restrictive rules are evaluated first and the most general rules are evaluated last <a href="#">About the firewall rule, firewall setting, and intrusion prevention processing order</a></li><li>That the client uses stateful inspection, which keeps track of the state of the network connections <a href="#">How the firewall uses stateful inspection</a></li><li>The firewall components that make up the firewall rule</li></ul> <p>When you understand about these triggers and how you can best use them, you can customize your firewall rules to protect your clients and servers.</p> <p><a href="#">The elements of a firewall rule on the client</a></p>
Add a new firewall rule	<p>You can perform the following tasks to manage firewall rules:</p> <ul style="list-style-type: none"><li>Add new firewall rules through the console using several methods One method lets you add a blank rule that has default settings. The other method offers a wizard that guides you through creating a new rule. Add your own rules to the rules that Symantec Endpoint Protection installs by default <a href="#">Adding firewall rules on the client</a></li><li>Customize a rule by changing any of the firewall rule criteria</li><li>Export and import firewall rules from another firewall policy <a href="#">Exporting or importing firewall rules on the client</a></li><li>Copy and paste firewall rules</li></ul> <p>You can save time creating a new firewall rule by copying an existing rule that is similar to the rule that you want to create. Then you can modify the copied rule to meet your needs.</p>
Customize a firewall rule	<p>After you create a new rule, or if you want to customize a default rule, you can modify any of the firewall rule criteria.</p>

## Adding a new firewall rule

You can create new firewall rules using either of the following methods:

Blank rule	<p>A blank rule allows all traffic.</p> <p><a href="#">To add a new blank firewall rule</a></p>
<b>Add Firewall Rule</b> wizard	<p>If you add rules with the <b>Add Firewall Rule</b> wizard, ensure that you configure the rule. The wizard does not configure new rules with multiple criteria.</p> <p><a href="#">To add a firewall rule using a wizard</a></p>

You should specify both the inbound and the outbound traffic in the rule whenever possible. You do not need to create inbound rules for traffic such as HTTP. The Symantec Endpoint Protection client uses stateful inspection for TCP traffic. Therefore, it does not need a rule to filter the return traffic that the clients initiate.

When you create a new firewall rule, it is automatically enabled. You can disable a firewall rule if you need to allow specific access to a computer or application. The rule is disabled for all inherited policies.

The rule is also disabled for the all locations if it is a shared policy and only one location if it is a location-specific policy.

---

## NOTE

Rules must be enabled for the firewall to process them.

1. To add a new blank firewall rule, in the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Rules**.  
For versions earlier than 14.2, there is no option for **Mac Settings**.
3. On the **Rules** tab, under the **Rules** list, click **Add Blank Rule**.
4. Optionally, you can change the firewall rule criteria as needed.
5. If you are done with the configuration of the rule, click **OK**.
6. To add a firewall rule using a wizard, in the console, open a Firewall policy.
7. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Rules**.  
On the **Rules** tab, under the **Rules** list, click **Add Rule**.
8. Fill out the options on each screen, and then click **Next**.
9. Click **Finish**.

Optionally, you can change the firewall rule criteria as needed.

[Customizing firewall rules](#)

[How the firewall uses stateful inspection](#)

## About firewall server rules and client rules

Rules are categorized as either server rules or client rules. Server rules are the rules that you create in Symantec Endpoint Protection Manager and that are downloaded to the Symantec Endpoint Protection client. Client rules are the rules that the user creates on the client.

All rules on the Mac client are server rules. Mac users do not have the option of creating client rules for the Mac client.

The firewall was introduced in the Mac client as of version 14.2.

[User control level and rule status](#) describes the relationship between the client's user control level and the user's interaction with the firewall rules.

**Table 82: User control level and rule status**

User control level	User interaction
Server control	The Windows client receives server rules but the user cannot view them. The user cannot create client rules. The Mac client does not allow the user to enable or disable the firewall.
Mixed control	The Windows client receives server rules. The user can create client rules, which are merged with server rules and client security settings. The Mac client allows or disallows the user to enable or disable the firewall. It depends on whether the granular setting is set to server control or client control.
Client control	The client does not receive server rules. The user can create client rules. The Symantec Endpoint Protection Manager administrator cannot view client rules. The Mac client allows the user to enable or disable the firewall.

[Preventing users from disabling protection on client computers](#)



[Server rules and client rules processing priority](#) lists the order that the firewall processes server rules, client rules, and client settings.

**Table 83: Server rules and client rules processing priority**

Priority	Rule type or setting
First	Server rules with high priority levels (rules above the blue line in the <b>Rules</b> list)
Second	Client rules
Third	Server rules with lower priority levels (rules under the blue line in the <b>Rules</b> list) On the client, server rules under the blue line are processed after client rules.
Fourth	Client security settings
Fifth	Client application-specific settings

On the client, users can modify a client rule or security setting, but users cannot modify a server rule.

**WARNING**

If the client is in mixed control, users can create a client rule that allows all traffic. This rule overrides all server rules under the blue line.

[Managing firewall rules](#)

[Changing the order of firewall rules](#)

[Preventing users from disabling protection on client computers](#)

## About the firewall rule, firewall setting, and intrusion prevention processing order

Firewall rules are ordered sequentially, from highest to lowest priority in the rules list. If the first rule does not specify how to handle a packet, the firewall inspects the second rule. This process continues until the firewall finds a match. After the firewall finds a match, the firewall takes the action that the rule specifies. Subsequent lower priority rules are not inspected. For example, if a rule that blocks all traffic is listed first, followed by a rule that allows all traffic, the client blocks all traffic.

You can order rules according to exclusivity. The most restrictive rules are evaluated first, and the most general rules are evaluated last. For example, you should place the rules that block traffic near the top of the rules list. The rules that are lower in the list might allow the traffic.

The Rules list contains a blue dividing line. The dividing line sets the priority of rules in the following situations:

- When a subgroup inherits rules from a parent group.
- When the Windows client is set to mixed control. The firewall processes both server rules and client rules.

The best practices for creating a rule base include the following order of rules:

1st	Rules that block all traffic.
2nd	Rules that allow all traffic.
3rd	Rules that allow or block specific computers.
4th	Rules that allow or block specific applications, network services, and ports.

[Processing order](#) shows the order in which the firewall processes the rules, firewall settings, and intrusion prevention settings.

**Table 84: Processing order**

Priority	Setting
First	Custom IPS signatures
Second	Intrusion Prevention settings, traffic settings, and stealth settings
Third	Built-in rules
Fourth	Firewall rules
Fifth	Port scan checks
Sixth	IPS signatures that are downloaded through LiveUpdate

## About inherited firewall rules

A subgroup's policy can inherit only the firewall rules that are enabled in the parent group. When you have inherited the rules, you can disable them, but you cannot modify them. As the new rules are added to the parent group's policy, the new rules are automatically added to the inheriting policy.

When the inherited rules appear in the **Rules** list, they are shaded in italics. Above the blue line, the inherited rules are added above the rules that you created as Symantec Endpoint Protection Manager administrator. Below the blue line, the inherited rules are added below the rules that you created.

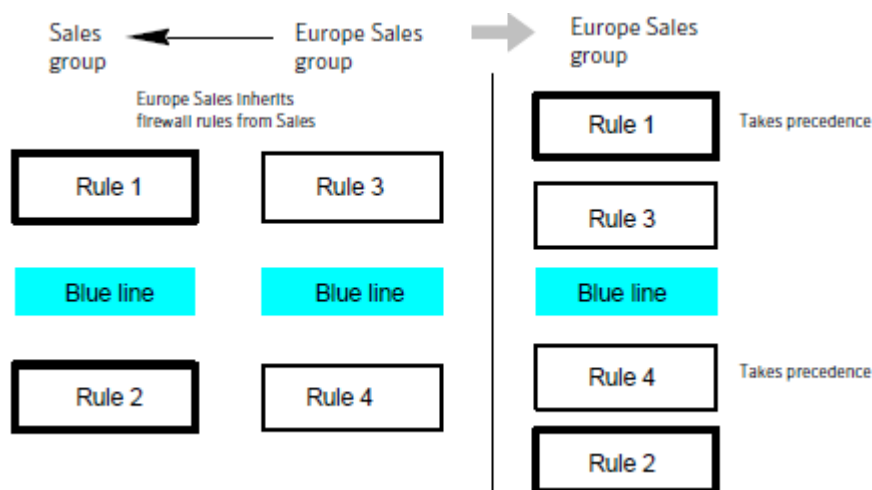
A Firewall policy also inherits default rules, so the subgroup's Firewall policy may have two sets of default rules. You may want to delete one set of default rules.

If you want to remove the inherited rules, you remove the inheritance rather than delete them. You have to remove all the inherited rules rather than the selected rules.

The firewall processes inherited firewall rules in the **Rules** list as follows:

Above the blue dividing line	The rules that the policy inherits take precedence over the rules that you create.
Below the blue dividing line	The rules that you create take precedence over the rules that the policy inherits.

The following figure shows how the **Rules** list orders rules when a subgroup inherits rules from a parent group. In this example, the Sales group is the parent group. The Europe Sales group inherits from the Sales group.



---

## [Managing firewall rules](#)

### [Adding inherited firewall rules from a parent group](#)

## **Adding inherited firewall rules from a parent group**

You can add firewall rules to a firewall policy by inheriting rules from a parent group. To inherit the rules from a parent group, the subgroup's policy must be a non-shared policy.

### **NOTE**

If the group inherits all of its policies from a parent group, this option is unavailable.

To add inherited firewall rules from a parent group

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Rules**.

For versions earlier than 14.2, there is no option for **Mac Settings**.

3. On the **Rules** tab, check **Inherit Firewall Rules from Parent Group**.

To remove the inherited rules, uncheck **Inherit Firewall Rules from Parent Group**.

4. Click **OK**.

### [Editing a policy](#)

### [About inherited firewall rules](#)

### [Managing firewall rules](#)

## **Changing the order of firewall rules**

The firewall processes the list of firewall rules from the top down. You can determine how the firewall processes firewall rules by changing their order.

If the Symantec Endpoint Protection client uses location switching, when you change the firewall rule order, the change affects the order for the current location only.

### **NOTE**

For better protection, place the most restrictive rules first and the least restrictive rules last.

### [About the firewall rule, firewall setting, and intrusion prevention processing order](#)

To change the order of firewall rules

1. In the console, open a Firewall policy.
2. In the **Firewall Policy** page, click **Rules**, and then select the rule that you want to move.
3. Do one of the following tasks:
  - To process this rule before the previous rule, click **Move Up**.
  - To process this rule after the rule below it, click **Move Down**.
4. Click **OK**.

To change the order of a firewall rule

- 
5. In the client, in the sidebar, click **Status**.
  6. Beside **Network and Host Exploit Mitigation**, click **Options > Configure Firewall Rules**
  7. In the **Configure Firewall Rules** dialog box, select the rule that you want to move.
  8. Do one of the following actions:
    - To have the firewall process this rule before the rule above it, click the up arrow.
    - To have the firewall process this rule after the rule below it, click the down arrow.
  9. When you finish moving rules, click **OK**.

## Managing firewall rules

### How the firewall uses stateful inspection

Firewall protection uses stateful inspection to track current connections. Stateful inspection tracks source and destination IP addresses, ports, applications, and other connection information. Before the client inspects the firewall rules, it makes the traffic flow decisions that are based on the connection information.

For example, if a firewall rule allows a computer to connect to a Web server, the firewall logs the connection information. When the server replies, the firewall discovers that a response from the Web server to the computer is expected. It permits the Web server traffic to flow to the initiating computer without inspecting the rule base. A rule must permit the initial outbound traffic before the firewall logs the connection.

Stateful inspection eliminates the need to create new rules. For the traffic that is initiated in one direction, you do not have to create the rules that permit the traffic in both directions. The client traffic that is initiated in one direction includes Telnet (port 23), HTTP (port 80), and HTTPS (port 443). The client computers initiate this outbound traffic; you create a rule that permits the outbound traffic for these protocols. Stateful inspection automatically permits the return traffic that responds to the outbound traffic. Because the firewall is stateful in nature, you only need to create the rules that initiate a connection, not the characteristics of a particular packet. All packets that belong to an allowed connection are implicitly allowed as being an integral part of that same connection.

Stateful inspection supports all rules that direct TCP traffic.

Stateful inspection does not support the rules that filter ICMP traffic. For ICMP traffic, you must create the rules that permit the traffic in both directions. For example, for the clients to use the ping command and receive replies, you must create a rule that permits ICMP traffic in both directions.

The state table that maintains the connection information may be periodically cleared. For example, it is cleared when a Firewall policy update is processed or if Symantec Endpoint Protection services are restarted.

### About firewall rule application triggers

When the application is the only trigger you define in a rule that allows traffic, the firewall allows the application to perform any network operation. The application is the significant value, not the network operations that the application performs. For example, suppose you allow Internet Explorer and you define no other triggers. Users can access the remote sites that use HTTP, HTTPS, FTP, Gopher, and any other protocol that the Web browser supports. You can define additional triggers to describe the particular network protocols and hosts with which communication is allowed.

Application-based rules may be difficult to troubleshoot because an application may use multiple protocols. For example, if the firewall processes a rule that allows Internet Explorer before a rule that blocks FTP, the user can still communicate with FTP. The user can enter an FTP-based URL in the browser, such as ftp://ftp.symantec.com.

For example, suppose you allow Internet Explorer and define no other triggers. Computer users can access the remote sites that use HTTP, HTTPS, FTP, Gopher, and any other protocol that the Web browser supports. You can define additional triggers to describe the network protocols and hosts with which communication is allowed.

---

You should not use application rules to control traffic at the network level. For example, a rule that blocks or limits the use of Internet Explorer would have no effect should the user use a different Web browser. The traffic that the other Web browser generates would be compared against all other rules except the Internet Explorer rule. Application-based rules are more effective when the rules are configured to block the applications that send and receive traffic.

[Defining information about applications](#)

[Notifying the users that access to an application is blocked](#)

[Managing firewall rules](#)

[Blocking networked applications that might be under attack](#)

## Defining information about applications

You can define information about the applications that clients run and include this information in a firewall rule.

**You can define applications in the following ways:**

- Type the information manually.  
[To define information about applications manually](#)
  - Search for the application in the learned applications list.  
Applications in the learned applications list are the applications that client computers in your network run.  
[To search for applications from the learned applications list](#)
1. To define information about applications manually, in the console, open a Firewall policy.
  2. On the **Firewall Policies** page, under **Windows Settings**, click **Rules**.  
For versions earlier than 14.2, on the **Firewall Policies** page, click **Rules**.
  3. On the **Rules** tab, in the **Rules** list, right-click the **Application** field for the rule you want to change, and then click **Edit**.
  4. In the **Application List** dialog box, click **Add**.
  5. In the **Add Application** dialog box, enter one or more of the following fields:
    - File name, which can include the file path
    - File description  
This field is used for display purposes only. It does not function as a matching condition.
    - File size, in bytes
    - Date that the application was last changed
    - File fingerprint

### NOTE

Network Application Monitoring must be enabled to define a firewall rule by file size, date last modified, or file fingerprint. If Network Application Monitoring is disabled, rule processing ignores all fields except for **File Name**.

- 
6. Click **OK** to add the application conditions.
  7. Click **OK** to save the application list.
  8. To search for applications from the learned applications list, on the **Firewall Policies** page, click **Rules**.
  9. On the **Rules** tab, select a rule, right-click the **Application** field, and then click **Edit**.
  10. In the **Application List** dialog box, click **Add From**.
  11. In the **Search for Applications** dialog box, search for an application.
  12. Under the **Query Results** table, to add the application to the **Applications** list, select the application, click **Add**, and then click **OK**.
  13. Click **Close**.
  14. Click **OK**.

[Managing firewall rules](#)

[Editing a policy](#)

[About firewall rule application triggers](#)

## Blocking networked applications that might be under attack

Network application monitoring tracks an application's behavior in the security log. If an application's content is modified too frequently, it is likely that a Trojan horse attacked the application and the client computer is not safe. If an application's content is modified on an infrequent basis, it is likely that a patch was installed and the client computer is safe. You can use this information to create a firewall rule that allows or blocks an application.

You can configure the client to detect and monitor any application that runs on the client computer and that is networked. Network applications send and receive traffic. The client detects whether an application's content changes.

If you suspect that a Trojan horse has attacked an application, you can use network application monitoring to configure the client to block the application. You can also configure the client to ask users whether to allow or block the application.

### An application's content changes for the following reasons:

- A Trojan horse attacked the application.
- The application was updated with a new version or an update.

You can add applications to a list so that the client does not monitor them. You may want to exclude the applications that you think are safe from a Trojan horse attack, but that have frequent and automatic patch updates.

You may also want to minimize the number of notifications that ask users to allow or block a network application.

To block networked applications that might be under attack

1. In the console, click **Clients**.
2. Under **Clients**, select a group, and then click **Policies**.
3. On the **Policies** tab, under **Location-independent Policies and Settings**, click **Network Application Monitoring**.
4. In the **Network Application Monitoring for group name** dialog box, click **Enable Network Application Monitoring**.
5. In the **When an application change is detected** drop-down list, select the action that the firewall takes on the application that runs on the client as follows:

<b>Ask</b>	Asks the user to allow or block the application.
<b>Block the traffic</b>	Blocks the application from running.

<b>Allow and Log</b>	Allows the application to run and records the information in the security log. The firewall takes this action on the applications that have been modified only.
----------------------	--

- If you selected **Ask**, click **Additional Text**.
- In the **Additional Text** dialog box, type the text that you want to appear under the standard message, and then click **OK**.
- To exclude an application from being monitored, under **Unmonitored Application List**, do one of the following tasks:

To define an application manually	Click <b>Add</b> , fill out one or more fields, and then click <b>OK</b> .
To define an application from a learned applications list	Click <b>Add From</b> . The learned applications list monitors both networked and non-networked applications. You must select networked applications only from the learned applications list. After you have added applications to the <b>Unmonitored Applications List</b> , you can enable, disable, edit, or delete them.

- Check the box beside the application to enable it; uncheck it to disable it.
- Click **OK**.

## Managing firewall rules

[Notifying the users that access to an application is blocked](#)

[About firewall rule application triggers](#)

[Searching for information about the applications that the computers run](#)

[Collecting information about the applications that the client computers run](#)

## Notifying the users that access to an application is blocked

You can send users a notification that an application that they want to access is blocked. This notification appears on the users' computers.

### NOTE

Enabling too many notifications can not only overwhelm your users, but can also alarm them. Use caution when enabling notifications.

To notify the users that access to an application is blocked

- In the console, open a Firewall policy.
- On the **Firewall Policies** page, click **Rules**.
- On the **Notifications** tab, check **Display notification on the computer when the client blocks an application** and optionally add a custom message.
- Click **OK**.

## Managing firewall rules

[Configuring client notifications for intrusion prevention and Memory Exploit Mitigation](#)

[Setting up administrator notifications](#)

## About firewall rule host triggers

You specify the host on both sides of the described network connection when you define host triggers.

Traditionally, the way to express the relationship between hosts is referred to as being either the source or destination of a network connection.

You can define the host relationship in either one of the following ways:

Source and destination	The source host and destination host are dependent on the direction of traffic. In one case the local client computer might be the source, whereas in another case the remote computer might be the source. The source and the destination relationship are more commonly used in network-based firewalls.
Local and remote	The local host is always the local client computer, and the remote host is always a remote computer that is positioned elsewhere on the network. This expression of the host relationship is independent of the direction of traffic. The local and the remote relationship is more commonly used in host-based firewalls, and is a simpler way to look at traffic.

You can define multiple source hosts and multiple destination hosts.

[The relationship between source and destination hosts](#) illustrates the source relationship and destination relationship with respect to the direction of traffic.



[The relationship between local and remote hosts](#) illustrates the local host and remote host relationship with respect to the direction of traffic.



Relationships are evaluated by the following types of statements:

The hosts that you define on either side of the connection (between the source and the destination)	OR statement
Selected hosts	AND statement

For example, consider a rule that defines a single local host and multiple remote hosts. As the firewall examines the packets, the local host must match the relevant IP address. However, the opposing sides of the address may be matched to any remote host. For example, you can define a rule to allow HTTP communication between the local host and either Yahoo.com or Google.com. The single rule is the same as two rules.

[Adding host groups](#)

[Blocking traffic to or from a specific server](#)

[Managing firewall rules](#)

## Adding host groups

A host group is a collection of: DNS domain names, DNS host names, IP addresses, IP ranges, MAC addresses, or subnets that are grouped under one name. The purpose of host groups is to eliminate the retyping of host addresses and names. For example, you can add multiple IP addresses one at a time to a firewall rule. Or, you can add multiple IP addresses to a host group, and then add the group to the firewall rule.

As you incorporate host groups, you must describe where the groups are used. If you decide later to delete a host group, you must first remove the host group from all the firewall rules that reference the group.

When you add a host group, it appears at the bottom of the **Hosts** list. You can access the **Hosts** list from the **Host** field in a firewall rule.

To add host groups



- 
1. In the console, click **Policies**.
  2. Expand **Policy Components**, and then click **Host Groups**.
  3. Under **Tasks**, click **Add a Host Group**.
  4. In the **Host Group** dialog box, type a name, and then click **Add**.
  5. In the **Host** dialog box, in the **Type** drop-down list, select a host.
  6. Type the appropriate information for each host type.
  7. Click **OK**.
  8. Add additional hosts, if necessary.
  9. Click **OK**.

[About firewall rule host triggers](#)

## About firewall rule network services triggers

Network services let networked computers send and receive messages, share files, and print. A network service uses one or more protocols or ports to pass through a specific type of traffic. For example, the HTTP service uses ports 80 and 443 in the TCP protocol. You can create a firewall rule that allows or blocks network services. A network service trigger identifies one or more network protocols that are significant in relation to the described network traffic.

When you define TCP-based or UDP-based service triggers, you identify the ports on both sides of the described network connection. Traditionally, ports are referred to as being either the source or the destination of a network connection.

[Adding network services to the default network services list](#)

[Permitting clients to browse for files and printers in the network](#)

[Managing firewall rules](#)

## Adding network services to the default network services list

Network services let networked computers send and receive messages, share files, and print. You can create a firewall rule that allows or blocks network services.

The network services list eliminates the need to retype protocols and ports for the firewall rules that you create to block or allow network services. When you create a firewall rule, you can select a network service from a default list of commonly used network services. You can also add network services to the default list. However, you need to be familiar with the type of protocol and the ports that it uses.

### NOTE

IPv4 and IPv6 are the two network layer protocols that are used on the Internet. If you install the client on the computers that run Windows Vista, the **Rules** list includes several default rules that block the Ethernet protocol type of IPv6. If you remove the default rules, you must create a rule that blocks IPv6.

### NOTE

You can add a custom network service through a firewall rule. However, that network service is not added to the default list. You cannot access the custom network service from any other rule.

To add network services to the default network services list

- 
1. In the console, click **Policies**.
  2. Expand **Policy Components**, and then click **Network Services**.
  3. Under **Tasks**, click **Add a Network Service**.
  4. In the **Network Service** dialog box, type a name for the service, and then click **Add**.
  5. Select a protocol from the **Protocol** drop-down list.  
The options change based on which protocol you select.
  6. Type in the appropriate fields, and then click **OK**.
  7. Add one or more additional protocols, as necessary.
  8. Click **OK**.

#### [Managing firewall rules](#)

#### [About firewall rule network services triggers](#)

#### [Controlling whether networked computers can share messages, files, and printing](#)

#### [Permitting clients to browse for files and printers in the network](#)

### **About firewall rule network adapter triggers**

You can define a firewall rule that blocks or allows traffic that passes through (transmitted or received) a network adapter.

When you define a particular type of adapter, consider how that adapter is used. For example, if a rule allows outbound HTTP traffic from Ethernet adapters, then HTTP is allowed through all the installed adapters of the same type. The only exception is if you also specify local host addresses. The client computer may use multi-NIC servers and the workstations that bridge two or more network segments. To control traffic relative to a particular adapter, the address scheme of each segment must be used rather than the adapter itself.

The network adapter list eliminates the need to retype types of adapters for firewall rules. Instead, when you create a firewall rule, you can select a network adapter from a default list of commonly used network adapters. You can also add network adapters to the default list.

You can select a network adapter from a default list that is shared across firewall policies and rules. The most common adapters are included in the default list in the **Policy Components** list.

#### **NOTE**

You can add a custom network adapter through a firewall rule. However, that network adapter is not added to the default list. You cannot access the custom network adapter from any other rule.

#### [Managing firewall rules](#)

#### [Adding a custom network adapter to the network adapter list](#)

#### [Controlling the traffic that passes through a network adapter](#)

### **Adding a custom network adapter to the network adapter list**

You can apply a separate firewall rule to each network adapter. For example, you may want to block traffic through a VPN at an office location, but not at a home location.

You can select a network adapter from a default list that is shared across firewall policies and rules. The most common adapters are included in the default list in the **Policy Components** list. Use the default list so that you do not have to retype each network adapter for every rule that you create.

---

The network adapter list eliminates the need to retype adapters for firewall rules. When you create a firewall rule, you can select a network adapter from a default list of commonly used network adapters. You can also add network adapters to the default list.

#### NOTE

You can add a custom network adapter through a firewall rule. However, that network adapter is not added to the default list. You cannot access the custom network adapter from any other rule.

To add a custom network adapter to the network adapter list

1. In the console, click **Policies > Policy Components > Network Adapters**.
2. Under **Tasks**, click **Add a Network Adapter**.
3. In the **Network Adapter** dialog box, in the **Adapter Type** drop-down list, select an adapter.
4. In the **Adapter Name** field, optionally type a description.
5. In the **Adapter Identification** text box, type the case-sensitive brand name of the adapter.

To find the brand name of the adapter, open a command line on the client, and then type the following text:

```
ipconfig/all
```

6. Click **OK**.

[Managing firewall rules](#)

[About firewall rule network adapter triggers](#)

[Controlling the traffic that passes through a network adapter](#)

## Importing and exporting firewall rules

You can export and import firewall rules and settings from another Firewall policy so that you do not have to re-create them. For example, you can import a partial rule set from one policy into another. To import rules, you first have to export the rules to a .dat file and have access to the file.

The rules are added in the same order that they are listed in the parent policy with respect to the blue line. You can then change their processing order.

1. To export firewall rules, in the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Rules**.

For versions earlier than 14.2, there is no option for **Mac Settings**.

3. In the **Rules** list, select the rules you want to export, right-click, and then click **Export**.
4. In the **Export Policy** dialog box, locate a directory to save the .dat file, type a file name, and then click **Export**.
5. To import firewall rules, in the console, open a Firewall policy.
6. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Rules**.

For versions earlier than 14.2, there is no option for **Mac Settings**.

- 
7. Right-click the Rules list, and then click **Import**.
  8. In the **Import Policy** dialog box, locate the .dat file that contains the firewall rules to import, and then click **Import**.
  9. In the **Input** dialog box, type a new name for the policy, and then click **OK**.
  10. Click **OK**.

[Adding a new firewall rule](#)

[Customizing firewall rules](#)

[About the firewall rule, firewall setting, and intrusion prevention processing order](#)

## Importing or exporting firewall rules on the client

You can share the rules with another Symantec Endpoint Protection client so that you do not have to recreate them. You can export the rules from another computer and import them into your computer. When you import rules, they are added to the bottom of the firewall rules list. Imported rules do not overwrite existing rules, even if an imported rule is identical to an existing rule.

The exported rules and imported rules are saved in a .sar file.

### To export firewall rules on the client:

1. In the client, in the sidebar, click **Status**.
2. Beside **Network and Host Exploit Mitigation**, click **Options > Configure Firewall Rules**.
3. In the **Configure Firewall Rules** dialog box, select the rules you want to export.
4. Right-click the rules, and then click **Export Selected Rules**.
5. In the **Export** dialog box, type a file name, and then click **Save**.
6. Click **OK**.

### To import firewall rules on the client:

1. In the client, in the sidebar, click **Status**.
2. Beside **Network and Host Exploit Mitigation**, click **Options > Configure Firewall Rules**.
3. In the **Configure Firewall Rules** dialog box, right-click the firewall rules list, and then click **Import Rule**.
4. In the **Import** dialog box, locate the file in .sar format that contains the rules you want to import.
5. Click **Open**.
6. Click **OK**.

## Customizing firewall rules

When you create a new Firewall policy, the policy includes several default rules. You can modify one or multiple rule components as needed.

The components of a firewall rule are as follows:

Actions	<p>The action parameters specify what actions the firewall takes when it successfully matches a rule. If the rule matches and is selected in response to a received packet, the firewall performs all actions. The firewall either allows or blocks the packet and logs or does not log the packet. If the firewall allows traffic, it lets the traffic that the rule specifies access the network. If the firewall blocks traffic, it blocks the traffic that the rule specifies so that it does not access the network.</p> <p><b>The actions are as follows:</b></p> <ul style="list-style-type: none"><li>• Allow The firewall allows the network connection.</li><li>• Block The firewall blocks the network connection.</li></ul> <p><b>Note:</b> The Mac client firewall monitors packets but does not log them.</p> <p><b>Note:</b> This note applies only as of 14.2.</p>
Triggers	<p>When the firewall evaluates the rule, all the triggers must be true for a positive match to occur. If any one trigger is not true in relation to the current packet, the firewall cannot apply the rule. You can combine the trigger definitions to form more complex rules, such as to identify a particular protocol in relation to a specific destination address.</p> <p><b>The triggers are as follows:</b></p> <ul style="list-style-type: none"><li>• Application When the application is the only trigger you define in an allow-traffic rule, the firewall allows the application to perform any network operation. The application is the significant value, not the network operations that the application performs. You can define additional triggers to describe the particular network protocols and hosts with which communication is allowed. <a href="#">About firewall rule application triggers</a></li><li>• Host When you define host triggers, you specify the host on both sides of the described network connection. Traditionally, the way to express the relationship between hosts is referred to as being either the source or destination of a network connection. <a href="#">About firewall rule host triggers</a></li><li>• Network services A network services trigger identifies one or more network protocols that are significant in relation to the described traffic. The local host computer always owns the local port, and the remote computer always owns the remote port. This expression of the port relationship is independent of the direction of traffic. <a href="#">About firewall rule network services triggers</a></li><li>• Network adapter If you define a network adapter trigger, the rule is relevant only to the traffic that is transmitted or received by using the specified type of adapter. You can specify either any adapter or the one that is currently associated with the client computer. <a href="#">About firewall rule network adapter triggers</a></li></ul>
Conditions	<p>Rule conditions consist of the rule schedule and screen saver state.</p> <p>The conditional parameters do not describe an aspect of a network connection. Instead, the conditional parameters determine the active state of a rule. You may define a schedule or identify a screen saver state that dictates when a rule is considered to be active or inactive. The conditional parameters are optional and if not defined, not significant. The firewall does not evaluate inactive rules.</p>
Notifications	<p>The Log settings let you specify whether the server creates a log entry or sends an email message when a traffic event matches the criteria that are set for this rule.</p> <p>The Severity setting lets you specify the severity level of the rule violation.</p>

To customize firewall rules

- 
1. In the console, open a Firewall policy.
  2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Rules**.  
For versions earlier than 14.2, there is no option for **Mac Settings**.
  3. On the **Rules** tab, in the **Rules** list, in the **Enabled** field, ensure that the box is checked to enable the rule; uncheck the box to disable the rule.  
Symantec Endpoint Protection only processes the rules that you enable. All rules are enabled by default.
  4. Double-click the **Name** field and type a unique name for the firewall rule.
  5. Right-click the **Action** field and select the action that you want Symantec Endpoint Protection to take if the rule is triggered.
  6. In the **Application** field, define an application.  
[Defining information about applications](#)
  7. In the **Host** field, specify a host trigger.  
[Blocking traffic to or from a specific server](#)
  8. In addition to specifying a host trigger, you can also specify the traffic that is allowed to access your local subnet.  
[Allowing only specific traffic to the local subnet](#)
  9. In the **Service** field, specify a network service trigger.  
[Controlling whether networked computers can share messages, files, and printing](#)
  10. In the **Log** field, specify when you want Symantec Endpoint Protection to send an email message to you when this firewall rule is violated.  
[Setting up notifications for firewall rule violations](#)
  11. Right-click the **Severity** field and select the severity level for the rule violation.
  12. In the **Adapter** column, specify an adapter trigger for the rule.  
[Controlling the traffic that passes through a network adapter](#)
  13. In the **Time** column, specify the time periods in which this rule is active.
  14. Right-click the **Screen Saver** field and specify the state that the client computer's screen saver must be in for the rule to be active.  
The **Created At** field is not editable. If the policy is shared, the term Shared appears. If the policy is not shared, the field shows the name of the group to which that the non-shared policy is assigned.
  15. Right-click the **Description** field, click **Edit**, type an optional description for the rule, and then click **OK**.
  16. If you are done with the configuration of the rule, click **OK**.

[Adding a new firewall rule](#)

[Managing firewall rules](#)

### **Blocking traffic to or from a specific server**

To block traffic to or from a specific server, you can block the traffic by IP address rather than by domain name or host name. Otherwise, the user may be able to access the IP address equivalent of the host name.

To block traffic to or from a specific server

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page, click **Rules**.
3. On the **Rules** tab, in the **Rules** list, select the rule you want to edit, right-click the **Host** field, and then click **Edit**.
4. In the **Host List** dialog box, do one of the following actions:
  - Click **Source/Destination**.
  - Click **Local/Remote**.
5. Do one of the following tasks:

To select a host type from the <b>Type</b> drop-down list	<b>Do all of the following tasks:</b> <ul style="list-style-type: none"> <li>• In the <b>Source and Destination</b> or <b>Local and Remote</b> tables, click <b>Add</b>.</li> <li>• In the <b>Host dialog</b> box, select a host type from the <b>Type</b> drop-down list, and type the appropriate information for each host type.</li> <li>• Click <b>OK</b>.</li> </ul> The host that you created is automatically enabled.
To select a host group	<b>In the Host List dialog box, do one of the following actions:</b> <ul style="list-style-type: none"> <li>• Click <b>Source/Destination</b>.</li> <li>• Click <b>Local/Remote</b>.</li> </ul> Then in the <b>Host List</b> dialog box, check the box in the <b>Enabled</b> column for any host group that you want to add to the rule.

6. Add additional hosts, if necessary.
7. Click **OK** to return to the **Rules** list.

[Adding a new firewall rule](#)

[Customizing firewall rules](#)

[Adding host groups](#)

## Allowing only specific traffic to the local subnet

You can create a firewall rule that permits only specific traffic to your local subnet. This firewall rule always applies to your local subnet IP address, regardless of what the address is. Therefore, even if you change your local subnet IP address, you never have to modify this rule for the new address.

For example, you can create this rule to permit traffic to port 80 only on the local subnet, regardless of what the local subnet IP address is.

To allow only specific traffic to the local subnet

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Rules**.  
For versions earlier than 14.2, there is no option for **Mac Settings**.
3. On the **Rules** tab, in the **Firewall Rules** table, find the rule that you want to edit.
4. Double-click in the **Host** column for the rule for which you want to create a local subnet traffic condition.
5. Under the type of hosts for which this rule applies (Local or Remote), click **Add**.
6. Click the **Address Type** drop-down list and select one of the following:
  - Windows: **Local Subnet**
  - Mac: **Subnet**

7. Click **OK**, and then click **OK** again to close out of the **Host List** dialog box.

Customizing firewall rules

Controlling whether networked computers can share messages, files, and printing

Network services let networked computers send and receive messages, shared files, and print. You can create a firewall rule that allows or blocks network services.

You can add a custom network service through a firewall rule. However, that network service is not added to the default list. You cannot access the custom service from any other rule.

- To control whether networked computers can share messages, files, and printing
1. In the console, open a Firewall policy.
  2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Rules**.

- For versions earlier than 14.2, there is no option for **Mac Settings**.
3. On the **Rules** tab, in the **Rules** list, select the rule you want to edit, right-click the **Service** field, and then click **Edit**.
  4. In the **Service List** dialog box, check the box beside each service that you want to trigger the rule.
  5. To add an additional service for the selected rule only, click **Add**.
  6. In the **Protocol** dialog box, select a protocol from the **Protocol** drop-down list.
  7. Fill out the appropriate fields.
  8. Click **OK**.
  9. Click **OK**.
  10. Click **OK**.

Adding a new firewall rule

Customizing firewall rules

About firewall rule network services triggers

Adding network services to the default network services list

Permitting clients to browse for files and printers in the network

You can enable the client to either share its files or to browse for shared files and printers on the local network. To prevent network-based attacks, you may not want to enable network file and printer sharing.

You enable network file and print sharing by adding firewall rules. The firewall rules allow access to the ports to browse and share files and printers. You create one firewall rule so that the client can share its files. You create a second firewall rule so that the client can browse for other files and printers.

The settings work differently based on the type of control that you specify for your client, as follows:

Client control or mixed control	Users on the Windows client can enable these settings automatically by configuring them in Network and Host Exploit Mitigation. Users on the Mac client can only enable or disable the firewall.
Mixed control	A server firewall rule that specifies this type of traffic can override these settings on Windows. All firewall rules are server firewall rules on a Mac.



Server control	These settings are not available on the client.
----------------	---

1. **Option 1:** To permit Windows clients to browse for files and printers in the network, in the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings**, click **Rules**.
3. On the **Rules** tab, in the **Rules** list, select the rule you want to edit, right-click the **Service** field, and then click **Edit**.
4. In the **Service List** dialog box, click **Add**.
5. In the **Protocol** dialog box, in the **Protocol** drop-down list, click **TCP**, and then click **Local/Remote**.
6. Do one of the following tasks:

To permit clients to browse for files and printers in the network	In the <b>Remote port</b> drop-down list, type 88, 135, 139, 445.
To enable other computers to browse files on the client	In the <b>Local Port</b> drop-down list, type 88, 135, 139, 445.

7. Click **OK**.
8. In the **Service List** dialog box, click **Add**.
9. In the **Protocol** dialog box, in the **Protocol** drop-down list, click **UDP**.
10. Do one of the following tasks:

To permit clients to browse for files and printers in the network	In the <b>Local Port</b> drop-down list, type 137, 138. In the <b>Remote Port</b> drop-down list, type 88.
To enable other computers to browse files on the client	In the <b>Local Port</b> drop-down list, type 88, 137, 138.

11. Click **OK**.
12. In the **Service List** dialog box, make sure that the two services are enabled, and then click **OK**.
13. On the **Rules** tab, make sure the **Action** field is set to **Allow**.
14. If you are done with the configuration of the policy, click **OK**.
15. **Option 2:** To permit Mac clients to browse for files and printers in the network, in the console, open a Firewall policy.

#### NOTE

The Mac firewall is available as of version 14.2.

16. On the **Firewall Policy** page, under **Mac Settings**, click **Rules**.
17. On the **Rules** tab, in the **Rules** list, select the rule you want to edit, right-click the **Service** field, and then click **Edit**.
18. In the **Service List** dialog box, click **Add**.
19. In the **Protocol** dialog box, in the **Protocol** drop-down list, click **TCP**, and then click **Local/Remote**.
20. To enable other computers to browse files on the client, in the **Local Port** drop-down list, type 139 and 445.  
Outgoing requests to browse the network from the Mac are enabled by default.

- 
- 21. Click **OK**.
  - 22. In the **Service List** dialog box, make sure that the new service is enabled, and then click **OK**.
  - 23. On the **Rules** tab, make sure the **Action** field is set to **Allow**.
  - 24. If you are done with the configuration of the policy, click **OK**.

Printer discovery on Macs is through the Bonjour service, which is open by default. You do not need to configure a custom rule for the Bonjour service.

[Adding a new firewall rule](#)  
[Customizing firewall rules](#)

**Setting up notifications for firewall rule violations**

You can configure Symantec Endpoint Protection to send you an email message each time the firewall detects a rule violation, attack, or event. For example, you may want to know when a client blocks the traffic that comes from a particular IP address.

- To set up notifications for firewall rule violations
- 1. In the console, open a Firewall policy.
  - 2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Rules**.  
For versions earlier than 14.2, there is no option for **Mac Settings**.
  - 3. On the **Rules** tab, select a rule, right-click the **Log** field, and do one or more of the following tasks:

To send an email message when a firewall rule is triggered	Check <b>Send Email Alert</b> .
To generate a log event when a firewall rule is triggered	For Windows rules, check both <b>Write to Traffic Log</b> and <b>Write to Packet Log</b> . For Mac rules, check <b>Write to Traffic Log</b> .

- 4. When you are done with the configuration of this policy, click **OK**.
- 5. Configure a security alert.
- 6. Configure a mail server.
- 7. Click **OK**.

[Adding a new firewall rule](#)  
[Customizing firewall rules](#)  
[Setting up administrator notifications](#)

**Controlling the traffic that passes through a network adapter**

When you define a network adapter trigger, the rule is relevant only to the traffic that the specified adapter transmits or receives.

You can add a custom network adapter from a firewall rule. However, that adapter is not added to the shared list. You cannot access the custom adapter from any other rule.

To control the traffic that passes through a network adapter

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings**, click **Rules**.
3. On the **Rules** tab, in the **Rules** list, select the rule you want to edit, right-click the **Adapter** field, and then click **More Adapters**.
4. In the **Network Adapter** dialog box, do one of the following actions:

To trigger the rule for any adapter (even if it is not listed)	Click <b>Apply the rule to all adapters</b> , and then go to step <a href="#">7</a> .
To trigger the rule for selected adapters	Click <b>Apply the rule to the following adapters</b> . Then check the box beside each adapter that you want to trigger the rule.

5. To add a custom adapter for the selected rule only, do the following tasks:
  - Click **Add**.
  - In the **Network Adapter** dialog box, select the adapter type and type the adapter's brand name in the **Adapter Identification** text field.
6. Click **OK**.
7. Click **OK**.
8. Click **OK**.

[Adding a new firewall rule](#)

[Customizing firewall rules](#)

[About firewall rule network adapter triggers](#)

## Configuring firewall settings for mixed control

You can configure the client so that users have no control, full control, or limited control over which firewall settings they can configure.

For the Mac firewall, the user cannot create firewall rules or change settings regardless of the client user interface settings. The options do not ever appear in the client user interface.

Server control	For Windows, the user cannot create any firewall rules or enable firewall settings. For Mac, the user cannot enable or disable the firewall.
Client control	For Windows, the user can create firewall rules and enable all firewall settings. For Mac, the user can enable and disable the firewall.
Mixed control	For Windows, the user can create firewall rules. You decide which firewall settings the user can enable. For Mac, you decide whether the user can enable or disable the firewall.

### NOTE

The firewall is only available for the Mac client as of version 14.2.

To configure firewall settings for mixed control

- 
1. In the console, click **Clients**.
  2. Under **Clients**, select the group with the user control level that you want to modify.
  3. On the **Policies** tab, under **Location-specific Policies and Settings**, under a location, expand **Location-specific Settings**.
  4. To the right of **Client User Interface Control Settings**, click **Tasks > Edit Settings**.
  5. In the **Control Mode Settings** dialog box, click **Mixed control**, and then click **Customize**.
  6. On the **Client/Server Control Settings** tab, under the **Firewall Policy** category, do one of the following tasks:
    - To make a client setting available for the users to configure, click **Client**.
    - To configure a client setting, click **Server**.
  7. Click **OK**.
  8. Click **OK**.
  9. For each firewall setting that you set to **Server**, enable or disable the setting in the Firewall policy.

### Managing firewall protection

#### Enabling communications for network services instead of adding a rule

## Enabling communications for network services instead of adding a rule

You can enable the options that automatically allow communication between certain network services so you do not have to define the rules that explicitly allow those services. You can also enable traffic settings to detect and block the traffic that communicates through NetBIOS and token rings.

You can allow outbound requests and inbound replies for the network connections that are configured to use DHCP, DNS, and WINS traffic.

The filters allow DHCP, DNS, or WINS clients to receive an IP address from a server. It also protects the clients against attacks from the network with the following conditions:

If the client sends a request to the server	The client waits for five seconds to allow an inbound response.
If the client does not send a request to the server	Each filter does not allow the packet.

When you enable these options, Symantec Endpoint Protection permits the packet if a request was made; it does not block packets. You must create a firewall rule to block packets.

### NOTE

To configure these settings in mixed control, you must also enable these settings in the **Client User Interface Mixed Control Settings** dialog box.

To enable communications for network services instead of adding a rule

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Built-in Rules**.

For versions earlier than 14.2, these settings are for Windows only.

- 
3. Check the options that you want to enable.
  4. Click **OK**.
  5. If you are prompted, assign the policy to a location.

[Creating a firewall policy](#)

[Editing a policy](#)

[Preventing users from disabling protection on client computers](#)

## Automatically blocking connections to an attacking computer

If the Symantec Endpoint Protection client detects a network attack, it can automatically block the connection to ensure that the client computer is safe. The client activates an Active Response, which automatically blocks all communication to and from the attacking computer for a set period of time. The IP address of the attacking computer is blocked for a single location.

The attacker's IP address is recorded in the Security log. You can unblock an attack by canceling a specific IP address or canceling all Active Response.

If you set the client to mixed control, you can specify whether the setting is available on the client for the user to enable. If it is not available, you must enable it in the **Client User Interface Mixed Control Settings** dialog box.

Updated IPS signatures, updated denial-of-service signatures, port scans, and MAC spoofing also trigger an Active Response.

To automatically block connections to an attacking computer

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page in the left pane, click one of the following options:
  - Under **Windows Settings: Protection and Stealth**
  - Under **Mac Settings: Protection**Mac settings are available only as of version 14.2.
3. Under **Protection Settings**, check **Automatically block an attacker's IP address**.
4. In the **Number of seconds during which to block IP address ... seconds** text box, specify the number of seconds to block potential attackers.

You can enter a value from 1 to 999,999.

5. Click **OK**.

[Creating a firewall policy](#)

[Configuring firewall settings for mixed control](#)

[Editing a policy](#)

## Detecting potential attacks and spoofing attempts

You can enable the various settings that enable Symantec Endpoint Protection to detect and log potential attacks on the client and block spoofing attempts. All of these options are disabled by default.

---

The settings that you can enable are as follows:

<b>Enable port scan detection</b>	When this setting is enabled, Symantec Endpoint Protection monitors all incoming packets that any security rule blocks. If a rule blocks several different packets on different ports in a short period of time, Symantec Endpoint Protection creates a Security log entry. Port scan detection does not block any packets. You must create a security policy to block traffic when a port scan occurs.
<b>Enable denial of service detection</b>	Denial of service detection is a type of intrusion detection. When enabled, the client blocks traffic if it detects a pattern from known signatures, regardless of the port number or type of Internet protocol.
<b>Enable anti-MAC spoofing</b>	When this setting is enabled, Symantec Endpoint Protection allows the following incoming and outgoing traffic if a request was made to that specific host: <ul style="list-style-type: none"><li>• Address resolution protocol (ARP) (IPv4)</li><li>• Neighbor Discovery Protocol (NDP) (IPv6)</li></ul> Supported as of version 14.2. All other unexpected traffic is blocked and an entry is generated to the Security log.

#### NOTE

To configure these settings in mixed control, you must also enable these settings in the **Client User Interface Mixed Control Settings** dialog box.

To detect potential attacks and spoofing attempts

1. In the console, open a Firewall policy.
2. In the **Firewall Policy** page, click one of the following:
  - Under **Windows Settings: Protection and Stealth**
  - Under **Mac Settings: Protection**Mac settings are available only as of version 14.2.
3. Under **Protection Settings**, check any of the options that you want to enable.
4. Click **OK**.
5. If you are prompted, assign the policy to a location.

[Creating a firewall policy](#)

[Preventing users from disabling protection on client computers](#)

[Editing a policy](#)

## Preventing outside stealth attacks on computers

You can enable the settings that prevent outside attacks from detecting information about your clients. These settings are disabled by default.

#### NOTE

To configure these settings in mixed control, you must also enable these settings in the **Client User Interface Mixed Control Settings** dialog box.

#### NOTE

These stealth settings are not available for the Mac firewall.

The firewall is included with the Mac client as of 14.2.

To prevent outside stealth attacks on computers

- 
1. In the console, open a Firewall policy.
  2. In the **Firewall Policy** page, click **Protection and Stealth**.
  3. Under **Stealth Settings**, check any of the options that you want to enable.
  4. Click **OK**.
  5. If you are prompted, assign the policy to a location.

[Creating a firewall policy](#)

[Preventing users from disabling protection on client computers](#)

[Editing a policy](#)

## Disabling the Windows Firewall

You can specify the conditions in which Symantec Endpoint Protection disables Windows Firewall. Symantec Endpoint Protection restores the Windows Firewall settings to the state it was in before Symantec Endpoint Protection was installed when the following occurs:

- Symantec Endpoint Protection is uninstalled.
- The Symantec Endpoint Protection firewall is disabled.

### NOTE

Symantec Endpoint Protection does not modify any existing Windows Firewall policy rules or exclusions.

Typically, a Windows user receives a notification when their computer restarts if Windows Firewall is disabled. Symantec Endpoint Protection disables this notification by default so that it does not alarm your users when Windows Firewall is disabled. However, you can enable the notification, if desired.

To disable the Windows Firewall

1. In the console, click **Policies**.
2. Under **Policies**, click **Firewall**.
3. Do one of the following tasks:
  - Create a new firewall policy.
  - In the **Firewall Policies** list, double-click on the firewall policy that you want to modify.
4. Under **Firewall Policy**, click **Windows Integration**.
5. In the **Disable Windows Firewall** drop-down list, specify when you want Windows Firewall disabled.

The default setting is **Disable Once Only**.

Click **Help** for more information on the options.

[Windows Integration](#)

6. In the **Windows Firewall Disabled Message** drop-down list, specify whether you want to disable the Windows message on startup to indicate that the firewall is disabled.

The default setting is **Disable**, which means the user does not receive a message upon a computer startup that Windows Firewall is disabled.

7. Click **OK**.

[Creating a firewall policy](#)

[The types of security policies](#)

---

## Managing intrusion prevention

The default intrusion prevention settings protect client computers against a wide variety of threats. You can change the default settings for your network.

If you run Symantec Endpoint Protection on servers, intrusion prevention might affect server resources or response time. For more information, see:

[Best practices for Endpoint Protection on Windows Servers](#)

### NOTE

The Linux client does not support intrusion prevention.

**Table 85: Managing intrusion prevention**

Task	Description
Learn about intrusion prevention	Learn how intrusion prevention detects and blocks network and browser attacks. <a href="#">How intrusion prevention works</a> <a href="#">About Symantec IPS signatures</a>
Enable intrusion prevention	To keep your client computers secure, you should keep intrusion prevention enabled: <ul style="list-style-type: none"><li>• Network intrusion prevention</li><li>• Browser intrusion prevention (Windows computers only)</li></ul> You can also configure browser intrusion prevention to only log detections, but not block them. You should use this configuration on a temporary basis as it lowers the client's security profile. For example, you would configure log-only mode only while you troubleshoot blocked traffic on the client. After you review the attack log to identify and exclude the signatures that block traffic, you disable log-only mode. <a href="#">Enabling network intrusion prevention or browser intrusion prevention</a> <a href="#">Creating exceptions for IPS signatures</a> You can also enable both types of intrusion prevention, as well as the firewall, when you run the <b>Enable Network Threat Protection</b> command on a group or client. <a href="#">Running commands on client computers from the console</a>



Task	Description
Create exceptions to change the default behavior of Symantec network intrusion prevention signatures	<p>You might want to create exceptions to change the default behavior of the default Symantec network intrusion prevention signatures. Some signatures block the traffic by default and other signatures allow the traffic by default.</p> <p><b>Note:</b> You cannot change the behavior of browser intrusion prevention signatures.</p> <p><b>You might want to change the default behavior of some network signatures for the following reasons:</b></p> <ul style="list-style-type: none"> <li>• Reduce consumption on your client computers. For example, you might want to reduce the number of signatures that block traffic. Make sure, however, that an attack signature poses no threat before you exclude it from blocking.</li> <li>• Allow some network signatures that Symantec blocks by default. For example, you might want to create exceptions to reduce false positives when benign network activity matches an attack signature. If you know the network activity is safe, you can create an exception.</li> <li>• Block some signatures that Symantec allows. For example, Symantec includes signatures for peer-to-peer applications and allows the traffic by default. You can create exceptions to block the traffic instead.</li> <li>• Use audit signatures to monitor certain types of traffic (Windows only) Audit signatures have a default action of <b>Not log</b> for certain traffic types, such as traffic from instant message applications. You can create an exception to log the traffic so that you can view the logs and monitor this traffic in your network. You can then use the exception to block the traffic, create a firewall rule to block the traffic, or leave the traffic alone. You can also create an application rule for the traffic.</li> </ul> <p><a href="#">Creating exceptions for IPS signatures</a> You can use application control to prevent users from running peer-to-peer applications on their computers.</p> <p><a href="#">Adding custom rules to Application Control</a> If you want to block the ports that send and receive peer-to-peer traffic, use a Firewall policy.</p> <p><a href="#">Creating a firewall policy</a></p>
Create exceptions to ignore browser signatures on client computers (Windows only)	<p>You can create exceptions to exclude browser signatures from browser intrusion prevention on Windows computers.</p> <p>You might want to ignore browser signatures if browser intrusion prevention causes problems with browsers in your network.</p> <p><a href="#">Creating exceptions for IPS signatures</a></p>
Exclude specific computers from network intrusion prevention scans	<p>You might want to exclude certain computers from network intrusion prevention. For example, some computers in your internal network may be set up for testing purposes. You might want Symantec Endpoint Protection to ignore the traffic that goes to and from those computers.</p> <p>When you exclude computers, you also exclude them from the denial of service protection and port scan protection that the firewall provides.</p> <p><a href="#">Setting up a list of excluded computers</a></p>
Configure intrusion prevention notifications	<p>By default, messages appear on client computers for intrusion attempts. You can customize the message.</p> <p><a href="#">Configuring client notifications for intrusion prevention and Memory Exploit Mitigation</a></p>
Create custom intrusion prevention signatures (Windows only)	<p>You can write your own intrusion prevention signature to identify a specific threat. When you write your own signature, you can reduce the possibility that the signature causes a false positive. For example, you might want to use custom intrusion prevention signatures to block and log websites.</p> <p><a href="#">Managing custom intrusion prevention signatures</a> You must have the firewall installed and enabled to use custom IPS signatures.</p> <p><a href="#">Choosing which security features to install on the client</a></p>
Monitor intrusion prevention	<p>Regularly check that intrusion prevention is enabled on the client computers in your network.</p> <p><a href="#">Monitoring endpoint protection</a></p>

---

## How intrusion prevention works

Intrusion prevention and the firewall are part of Network Threat Protection. As of version 14, Network Threat Protection and Memory Exploit Mitigation are part of Network and Host Exploit Mitigation.

Intrusion prevention automatically detects and blocks network attacks and attacks on browsers. Intrusion prevention is the second layer of defense after the firewall to protect client computers. Intrusion prevention is sometimes called the intrusion prevention system (IPS).

Intrusion prevention automatically detects and blocks network attacks. On Windows computers, intrusion prevention also detects and blocks browser attacks on supported browsers. Intrusion prevention is the second layer of defense after the firewall to protect client computers. Intrusion prevention is sometimes called the intrusion prevention system (IPS).

Intrusion prevention intercepts data at the network layer. It uses signatures to scan packets or streams of packets. It scans each packet individually by looking for the patterns that correspond to network attacks or browser attacks. Intrusion prevention detects attacks on operating system components and the application layer.

**Table 86: Types of intrusion prevention**

Type	Description
Network intrusion prevention	Network intrusion prevention uses signatures to identify attacks on client computers. For known attacks, intrusion prevention automatically discards the packets that match the signatures. You can also create your own custom network signatures in Symantec Endpoint Protection Manager. You cannot create custom signatures on the client directly; however, you can import custom signatures on the client. Custom signatures are supported on Windows computers only. <a href="#">About Symantec IPS signatures</a>
Browser intrusion prevention (Windows only) Browser intrusion prevention	Browser intrusion prevention monitors attacks on Internet Explorer and Firefox. Browser intrusion prevention is not supported on any other browsers. Firefox might disable the Symantec Endpoint Protection plug-in, but you can turn it back on. This type of intrusion prevention uses attack signatures as well as heuristics to identify attacks on browsers. For some browser attacks, intrusion prevention requires that the client terminate the browser. A notification appears on the client computer. For the latest information about the browsers that browser intrusion prevention protects, see: <a href="#">Supported browser versions for browser intrusion prevention</a> .

[Managing intrusion prevention](#)

[Configuring intrusion prevention](#)

## About Symantec IPS signatures

Symantec intrusion prevention signatures are installed on the client by default.

Intrusion prevention uses the Symantec signatures to monitor individual packets or streams of packets. For streams of packets, intrusion prevention can remember the list of patterns or partial patterns from previous packets. It can then apply this information to subsequent packet inspections.

Symantec signatures include signatures for network intrusion prevention, which are downloaded to the client as part of LiveUpdate content. For Mac computers, there are some additional network intrusion prevention signatures that are built into the software.

---

On Windows computers, LiveUpdate content also includes signatures for browser intrusion prevention.

Network intrusion prevention signatures	Network signatures match patterns of an attack that can crash applications or exploit the operating systems on your client computers. You can change whether a Symantec network signature blocks or allows traffic. You can also change whether or not Symantec Endpoint Protection logs a detection from a signature in the Security log.
Browser intrusion prevention signatures (Windows only)	Browser signatures match patterns of attack on supported browsers, such as script files that can crash the browser. You cannot customize the action or log setting for browser signatures, but you can exclude a browser signature. You can configure browser intrusion prevention to log the browser detections but not block them. This action helps you identify those browser signatures that you may need to exclude. After you create the signature exclusions, you disable log-only mode.

The Symantec Security Response team supplies the attack signatures. The intrusion prevention engine and the corresponding set of signatures are installed on the client by default. The signatures are part of the content that you update on the client.

You can view information about IPS signatures on the following Symantec website page:

[Attack Signatures](#)

For information about the built-in IPS signatures for Mac clients, see the following article:

[Built-in signatures for Symantec Endpoint Protection IPS for Mac](#)

[Creating exceptions for IPS signatures](#)

[Managing intrusion prevention](#)

## About custom IPS signatures

You can create your own IPS network signatures. These signatures are packet-based.

Unlike Symantec signatures, custom signatures scan single packet payloads only. However, custom signatures can detect attacks in the TCP/IP stack earlier than the Symantec signatures.

Packet-based signatures examine a single packet that matches a rule. The rule is based on various criteria, such as port, protocol, source or destination IP address, TCP flag number, or an application. For example, a custom signature can monitor the packets of information that are received for the string “phf” in GET / cgi-bin/phf? as an indicator of a CGI program attack. Each packet is evaluated for that specific pattern. If the packet of traffic matches the rule, the client allows or blocks the packet.

You can specify whether or not Symantec Endpoint Protection logs a detection from custom signatures in the Packet log.

### NOTE

You must have the firewall installed and enabled to use custom IPS signatures.

[Choosing which security features to install on the client](#)

Custom signatures are supported on Windows computers only.

[Managing custom intrusion prevention signatures](#)

## Creating exceptions for IPS signatures

You use exceptions to change the behavior of Symantec IPS signatures.

---

For Windows and Mac computers, you can change the action that the client takes when the IPS recognizes a network signature. You can also change whether the client logs the event in the Security log.

For Windows computers, you cannot change the behavior of Symantec browser signatures; unlike network signatures, browser signatures do not allow custom action and logging settings. However, you can create an exception for a browser signature so that clients ignore the signature.

#### NOTE

When you add a browser signature exception, Symantec Endpoint Protection Manager includes the signature in the exceptions list and automatically sets the action to **Allow** and the log setting to **Do Not Log**. You cannot customize the action or the log setting.

### Managing intrusion prevention

#### NOTE

To change the behavior of a custom IPS signature that you create or import, you edit the signature directly. Custom signatures are supported on Windows computers only.

To create an exception for IPS signatures

1. In the console, open an Intrusion Prevention policy.
2. Under **Windows Settings** or **Mac Settings**, click **Exceptions**, and then click **Add**.

#### NOTE

The signatures list populates with the latest LiveUpdate content that the management console downloaded. For Windows computers, the list appears blank if the management server has not yet downloaded the content. For Mac computers, the list always contains at least the built-in signatures, which are installed automatically on your Mac clients.

3. In the **Add Intrusion Prevention Exceptions** dialog box, do the following actions to filter the signatures:
  - (Windows only) To display only the signatures in a particular category, select an option from the **Show category** drop-down list. If you select **Browser Protection**, the signature action options automatically change to **Allow** and **Do Not Log**.
  - (Windows and Mac) To display the signatures that are classified with a particular severity, select an option from the **Show severity** drop-down list.
4. Select one or more signatures.

To make the behavior for all signatures the same, click **Select All**.
5. Click **Next**.
6. In the **Signature Action** dialog box, set the following options and then click **OK**.
  - Set **Action** to **Block** or **Allow**
  - Set **Log** to **Log the traffic** or **Do not log the traffic**.

#### NOTE

These options only apply to network signatures. For browser signatures, click **OK**.

If you want to revert the signature's behavior back to the original behavior, select the signature in the **Exceptions** list, and then click **Delete**.

7. Click **OK** to save the policy changes.

### Managing exceptions in Symantec Endpoint Protection

---

## Setting up a list of excluded computers

Excluded hosts are supported for network intrusion prevention only.

You can set up a list of computers for which the client does not match attack signatures or check for port scans or denial-of-service attacks. Network intrusion prevention and peer-to-peer authentication allow any source traffic from hosts in the excluded hosts list. However, network intrusion prevention and peer-to-peer authentication continue to evaluate any destination traffic to hosts in the list. The list applies to both inbound traffic and outbound traffic, but only to the source of the traffic. The list also applies only to remote IP addresses.

For example, you might exclude computers to allow an Internet service provider to scan the ports in your network to ensure compliance with their service agreements. Or, you might have some computers in your internal network that you want to set up for testing purposes.

### NOTE

You can also set up a list of computers that allows all inbound traffic and outbound traffic unless an IPS signature detects an attack. In this case, you create a firewall rule that allows all hosts.

To set up a list of excluded computers

1. In the console, open an Intrusion Prevention policy.
2. On the policy page, click **Intrusion Prevention**.
3. If not checked already, check **Enable excluded hosts** and then click **Excluded Hosts**.
4. In the **Excluded Hosts** dialog box, check **Enabled** next to any host group that you want to exclude from network intrusion prevention.

#### [Blocking traffic to or from a specific server](#)

5. To add the hosts that you want to exclude, click **Add**.
6. In the **Host** dialog box, in the drop-down list, select one of the following host types:
  - IP address
  - IP range
  - Subnet
7. Enter the appropriate information that is associated with the host type you selected.

For more information about these options, click **Help**.
8. Click **OK**.
9. Repeat [To add the hosts that you want to exclude, click Add.](#) and [Click OK.](#) to add additional devices and computers to the list of excluded computers.
10. To edit or delete any of the excluded hosts, select a row, and then click **Edit** or **Delete**.
11. Click **OK**.
12. When you finish configuring the policy, click **OK**.

## Enabling network intrusion prevention or browser intrusion prevention

Intrusion prevention is enabled by default. Typically, you should not disable either type of intrusion prevention.

You can enable a log-only mode for browser intrusion prevention to record what traffic it blocks without affecting the client user. You can then use the **Network and Host Exploit Mitigation** attack logs in Symantec Endpoint Protection Manager to create exceptions in the **Intrusion Prevention** policy to ignore specific browser signatures. You would then disable log-only mode.

---

## NOTE

To configure these settings in mixed control, you must also enable these settings in the **Client User Interface Mixed Control Settings** dialog box.

To enable network intrusion prevention or browser intrusion prevention

1. In the console, open an Intrusion Prevention policy.
2. On the policy page, click **Intrusion Prevention**.
3. Make sure the following options are checked:
  - **Enable Network Intrusion Prevention**  
You can also exclude particular computers from network intrusion prevention.  
[Setting up a list of excluded computers](#)
  - **Enable Browser Intrusion Prevention for Windows**
4. Click **OK**.

[Creating exceptions for IPS signatures](#)

[Managing intrusion prevention](#)

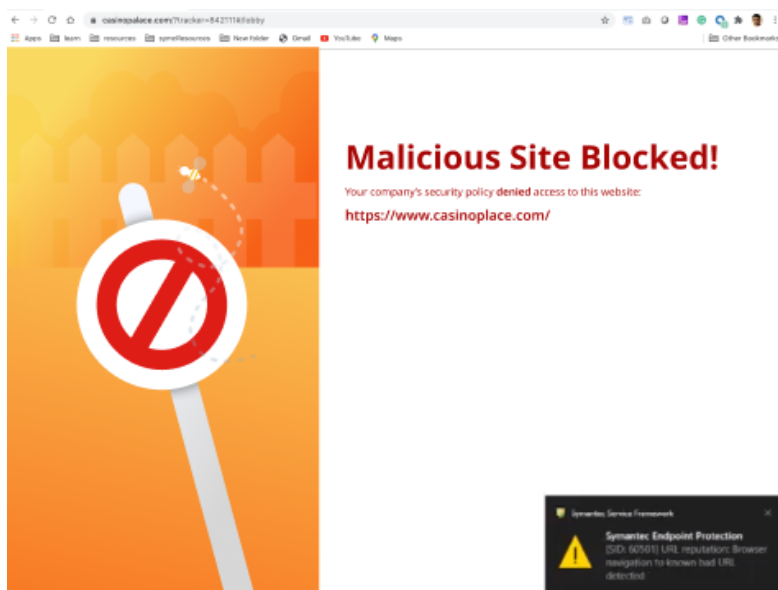
[Configuring firewall settings for mixed control](#)

## Integrating browser extensions with Symantec Endpoint Protection to protect against malicious websites

### What are browser extensions?

Browser extensions are plug-ins that add functionality and features to a web browser. Symantec Endpoint Protection (SEP) 14.3 RU2 and later installs a Google Chrome extension to protect client computers from accessing malicious websites. The Chrome browser extension monitors inbound and outbound HTTP and HTTPS traffic to the web browser and blocks the traffic if the client determines that the URL is malicious.

If the Chrome web browser detects that a URL is malicious, the client then redirects users to the following default landing page:



---

SEP protects client users accessing Mozilla Firefox and Microsoft Internet Explorer without using a browser extension. Instead, SEP supports these browsers based on the version of the Client Intrusion Detection System (CIDS) engine that the client uses.

### [Supported browsers for Browser Intrusion Prevention in Endpoint Protection](#)

All web browsers identify and protect malicious URLs using the following techniques:

- **Browser Intrusion Prevention** applies the IPS web browser signatures to the inbound and the outbound browser traffic on the client.  
[Expected behavior of Browser Intrusion Prevention](#)
- **URL reputation** identifies threats from domains and URLs that can host malicious content like malware, fraud, phishing, and spam. URL reputation then blocks access to the web addresses that are identified as known sources of the malicious content.  
[URL Reputation FAQ](#)

### **Installing the Chrome browser extension**

The Chrome browser extension is installed in one of the following ways:

1. The Symantec Endpoint Protection installer installs the Google Chrome browser extension by default. The SEP client modifies the local Local Group Policy (GPO) to enforce the browser extension.
2. If your organization uses Active Directory (AD) domains, you must configure AD Group Policy Object (GPO) policy to install the Chrome extension. If you use an AD GPO policy to manage your Chrome extensions, you must add the browser extension to your list. SEP then downloads the extension from the Google Web Store.  
You should use this option if you want to control the installation of the Chrome browser extension.

#### [Installing the Endpoint Protection Chrome Browser Extension using Group Policy Object](#)

##### **NOTE**

Items that you configure in the AD GPO policy have the highest priority over any installation method. If you install the SEP client first, the AD GPO policy overwrites the SEP client registry values. If you use the AD GPO policy first and the SEP client installs later, the client skips writing to the registry because it uses the Google Web Store URL.

In addition, when you deploy a client installation package, make sure that both the **Advanced Download Protection** and the **Intrusion Prevention** components are installed. The browser extension depends on IPS.

**Add Client Install Feature Set**

Name:

Description:

Feature sets for all previous versions are created automatically. You can also manually edit feature sets for previous versions.

Feature set version: 14.2 RU1 and later

<input checked="" type="checkbox"/> Virus, Spyware, and Basic Download Protection	Feature Description:
<input checked="" type="checkbox"/> Advanced Download Protection	Installs components for Intrusion Prevention.
<input type="checkbox"/> Microsoft Outlook Scanner	
<input checked="" type="checkbox"/> Proactive Threat Protection	
<input checked="" type="checkbox"/> SONAR Protection	Required component(s):
<input checked="" type="checkbox"/> Application and Device Control	
<input checked="" type="checkbox"/> Network and Host Exploit Mitigation	
<input checked="" type="checkbox"/> Firewall	
<input checked="" type="checkbox"/> Intrusion Prevention	
<input checked="" type="checkbox"/> Application Hardening	
<input checked="" type="checkbox"/> Endpoint Threat Defense for AD	The system will automatically install this component for you.
<input checked="" type="checkbox"/> Web and Cloud Access Protection	

If you upgrade the Chrome browser, the extension stays installed.

### How does the Chrome browser extension work?

After the Chrome browser extension is installed, LiveUpdate downloads a sub-feature of IPS, called WebExt. The browser extension uses WebExt definitions and IPS signatures.

WebExt definitions include the following components:

- **WebFilter:** Uses the extension engine WebPulse to inspect the URLs based on the domain and category. WebPulse uses Insight and reputation lookup.
- **Scanner:** A scan file that uses IPS signatures to report detections.

LiveUpdate automatically installs these definitions by default. Make sure this content is enabled by clicking **Admin > Servers > Edit Site Properties > LiveUpdate tab > Content Types to Download > Browser Extension**.

### Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager

One difference between the kernel IPS is that IPS cannot see HTTPS traffic, whereas the browser extension can.

### Configuring settings for the Chrome browser extension

After you install the Chrome web browser extension, make sure the following settings are enabled:

- (Required) In the Intrusion Prevention policy, enable **Enable Browser Intrusion Prevention for Windows** and **URL Reputation**. Both options are enabled by default.  
[Enabling network intrusion prevention or browser intrusion prevention](#)
- (Required) Make sure the IPS policy is enabled and assigned to the group. Browser protection depends on IPS.  
[Intrusion Prevention settings](#)
- (Optional) Create an exception to allow web domains so that the client never blocks them. In the Exceptions policy, add a Windows **Trusted Web Domain** exception.  
[Trusted Web Domain Exception](#)
- (Optional) If the Symantec Endpoint Protection Manager is enrolled in the cloud console, the Intensive Protection policy settings must be enabled.



### Logs and reports

#### How do I find browser attack detections?

On the SEP client, a detection displays the following possible Security log entries or notifications:

- Symantec Endpoint Protection [SID: 60501] URL Reputation Browser navigation to known bad URL blocked. <path>
- System Infected: PlugX Remote Access Tool Activity 2 attack blocked for this application: <path>
- [SID: 29565] Web Attack: Webpulse Bad Reputation Domain Request attack blocked. Traffic has been blocked for this application: <path>

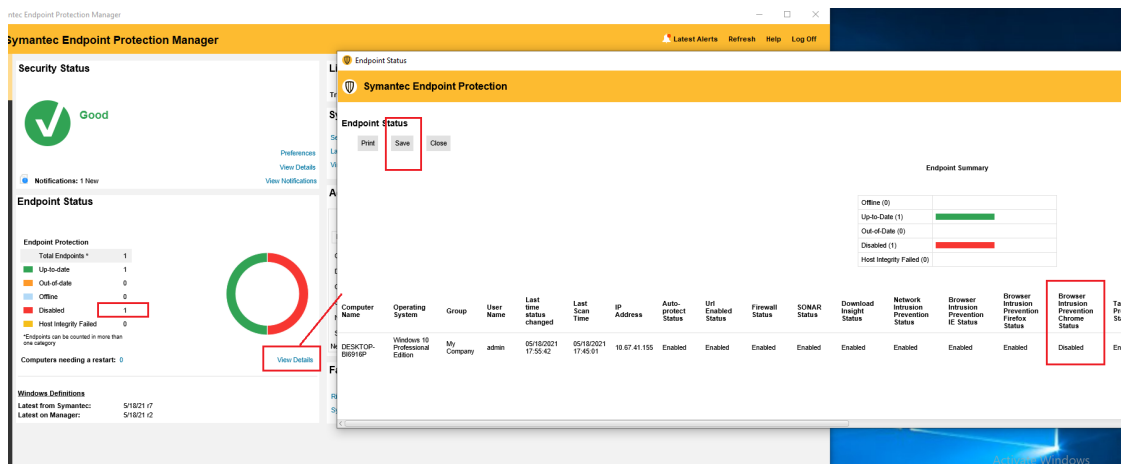
#### How do I find out whether the browser extensions are enabled?

The client displays information in the following locations:

- The **Clients** page > **Clients** tab > **Protection technology** view displays whether the browser extensions are enabled or disabled.
- The client System log displays an event every time that the browser extension is enabled or disabled, installed, or uninstalled, or removed from the browser.
- **Help** > **Troubleshooting** > **Versions** > **Browser Extension Engine** and **Browser Extension**.

The management server displays information in the following locations:

- On the **Home** page, under **Endpoint Status**, select the clients that have the **Disabled** status, and click **Details**. In the report, view the browser extensions that are enabled or disabled. Click **Save** to save the report in HTML format.



- On the **Home** page, under **Favorite Reports**, the **Symantec Endpoint Protection Weekly Status** report displays which clients have the extensions on or off.
- On the **Reports** > **Quick Reports** > **Computer Status** report type > **Protection Content Versions** report, click **Create Report**. Click the **Security Status Summary** report to see which clients have a disabled or malfunctioning browser extension, or updated browser extensions definitions.
- On the **Monitors** > **Logs** page, the Computer Status log displays columns for **IE Browser Protection Enabled**, **Firefox Browser Protection Enabled**, and **Chrome Browser Protection Enabled**. Click **Details** for the revision number for **Browser Extensions Definitions**. Use this information to make sure the browser extension content is downloaded to the client.

Symantec Endpoint Protection Manager

## Symantec Endpoint Protection Manager

Summary Logs Command Status Notifications

### Computer Status Logs

<< Back Export Details

Command: Scan

Computer	IP Address	Operating System	Infected	Auto-Protect
DESKTOP-BI6916P	10.67.41.155	Windows 10 Professional Edition	Not infected	Enabled

Reporting - Detailed Computer Information

Download Insight enabled: Enabled

Intrusion Prevention enabled: Enabled

Memory Exploit Mitigation enabled: Enabled

Early Launch Antimalware enabled: Enabled

IE Browser Protection enabled: Enabled

Firefox Browser Protection enabled: Enabled

Chrome Browser Protection enabled: Disabled

Tamper Protection enabled: Enabled

### Testing the Chrome browser extension

1. Paste the following URLs in a supported web browser to see if the browser blocks them. The browser may take several attempts.
2. Check the client **Security** log to see if the detections were logged.

[http://testrating.webfilter.bluecoat.com/Malicious%2520Sources/Malnets?locale=en\\_US](http://testrating.webfilter.bluecoat.com/Malicious%2520Sources/Malnets?locale=en_US)

[http://testrating.webfilter.bluecoat.com/Malicious%20Outbound%20Data/Botnets?locale=en\\_US](http://testrating.webfilter.bluecoat.com/Malicious%20Outbound%20Data/Botnets?locale=en_US)

[http://testrating.webfilter.bluecoat.com/Phishing?locale=en\\_US](http://testrating.webfilter.bluecoat.com/Phishing?locale=en_US)

<http://www.fakebook.com>

### Browser extension FAQs

#### Q: What are the Chrome versions that browser protection supports?

- Google Chrome (Linux, Mac, Windows): Version 9 and later
- Google Chrome OS: Version 11 and later

#### Supported browsers for Browser Intrusion Prevention in Endpoint Protection

#### Q: Do browser extensions use definitions?

Browser extension detections require Browser Extension definitions, SymPlatform definitions, and IPS definitions that Symantec LiveUpdate downloads.

#### About the types of content that LiveUpdate downloads

#### Q: Which IPS signatures are used for URL reputation detections?

- SID 60501 detections are for browser-based detections.
- SID 29565 detections are triggered from non-browser sources.

#### Q: How do I disable or uninstall the Chrome browser extension?

You should keep the Chrome browser extension installed and enabled for protection always. However, if you must troubleshoot issues with the browser, you can disable or uninstall the browser extension.

You can disable the browser extension in the following ways:

- Uncheck **Enable Browser Intrusion Prevention for Windows** in the IPS policy. The WebExt features such as the webFilter and scanner are disabled, but remain installed.

If you disable any part of the WebExt feature, it disables protection for the entire feature.

You can uninstall the Chrome browser extension in the following ways:

- Disable the IPS policy, which uninstalls extensions from all browsers.
- Uninstall the browser extension by removing the Google Chrome entry from the AD GPO policy.
- Uninstall the SEP client.
- Reinstall the SEP client without the Intrusion Prevention component.
- Run Cleanwipe. Cleanwipe uninstalls both the Symantec Endpoint Protection client and the Chrome browser extension.

## Troubleshooting

The following table displays the most common solutions that you might encounter when you install and might use the Chrome browser extension.

Steps	Description
Check the installation status of the browser extension	<p>On the management server computer:</p> <ul style="list-style-type: none"> <li>• Check that the following registry keys exist: <ul style="list-style-type: none"> <li>– HKEY_LOCAL_MACHINE\SOFTWARE\Google\Chrome\NativeMessagingHosts\com.broadcom.webextbridge</li> <li>– HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForcelist</li> <li>– HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Symantec\Symantec Endpoint Protection\{965393C7-9C7B-4B0A-BB01-CD0BC8425DEB}\Common Client\PathExpansionMap &gt; WebExtDefs\20210721.023</li> </ul> </li> </ul> <p>In the client computer:</p> <ul style="list-style-type: none"> <li>• Check that the WebExt folder and the updates.xml file exist: C:\ProgramData\Symantec\Symantec Endpoint Protection\14.3.4345.2000.105\Data\Definitions\WebExt\20210221.007\updates.xml</li> <li>• Check that the browser extension engine and definitions are enabled. Click <b>Help &gt; Troubleshooting &gt; Versions &gt; Browser Extension Engine and Browser Extension</b>.</li> </ul>
Check the installation status of the extension in Google Chrome	In the Google Chrome web browser, click the vertical ellipsis > <b>Settings &gt; Extensions &gt; Symantec Endpoint Protection &gt; Details</b> . Look for the <b>Version</b> number.
Run the Symantec Diagnostic (SymDiag) tool to collect: <ul style="list-style-type: none"> <li>• The.SDBZ file. The Symantec Diagnostic Tool takes a snapshot of your computer and logs the data in one file with an .SDBZ file extension.</li> <li>• The SymDiag tool logs information about unexpected detections in the WPP log.</li> </ul>	<p>To start the Symantec Diagnostic Tool, in the client, click <b>Help &gt; Download Symantec Diagnostic Tool</b>.</p> <p><a href="#">Collect data for support cases with Symantec Diagnostic Tool (SymDiag)</a></p>

## Known issues

- 
- If the Chrome Incognito mode is enabled (disabled by default), the client does not block malicious URLs. To disable this mode, in the Google Chrome web browser, click the vertical ellipsis > **Settings** > **Extensions** > **Symantec Endpoint Protection** > **Details**, and turn off **Allow in Incognito**.
  - The Chrome web browser may not block a malicious URL the first time a user accesses it. However, it blocks the URL after the second or third attempt. [SEP-70899]
  - If you add a Trusted Web Domain Exception URL using an IPv4 or IPv6 address, the Chrome extension does not recognize the address.
  - When you stop the client service, the Chrome browser extension still runs, but the client does not generate an event in the Security log.
  - As the Symantec Endpoint Protection client starts, the web extension runs. However, there is a short time period when the client does not generate any notifications or logs for an allowed or blocked URL. [MI-4947]

## Configuring client notifications for intrusion prevention and Memory Exploit Mitigation

By default, notifications appear on client computers when the client detects intrusion protection events and Memory Exploit Mitigation. When these notifications are enabled, they display a standard message. For IPS notifications, you can add customized text to the standard message.

To configure client notifications for intrusion prevention and Memory Exploit Mitigation

1. In the console, click **Clients** and under **Clients**, select a group.
2. On the **Policies** tab, under **Location-specific Policies and Settings**, under a location, expand **Location-specific Settings**.
3. To the right of **Client User Interface Control Settings**, click **Tasks**, and then click **Edit Settings**.
4. In the **Client User Interface Control Settings for group name** dialog box, click either **Server control** or **Mixed control**.
5. Beside **Mixed control** or **Server control**, click **Customize**.

If you click **Mixed control**, on the **Client/Server Control Settings** tab, beside **Show/Hide Intrusion Prevention notifications**, click **Server**. Then click the **Client User Interface Settings** tab.

6. In the **Client User Interface Settings** dialog box or tab, click **Display Intrusion Prevention and Memory Exploit Mitigation notifications**.
7. To enable a sound when the notification appears, click **Use sound when notifying users**.
8. Click **OK**.
9. Click **OK**.

[Managing intrusion prevention](#)

[Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy](#)

[Setting up administrator notifications](#)

## Managing custom intrusion prevention signatures

You can write your own network intrusion prevention signatures to identify a specific intrusion and reduce the possibility of signatures that cause a false positive. The more information you can add to a custom signature, the more effective the signature is.

---

## WARNING

You should be familiar with the TCP, UDP, or ICMP protocols before you develop intrusion prevention signatures. An incorrectly formed signature can corrupt the custom signature library and damage the integrity of the clients.

## NOTE

You must have the firewall installed and enabled to use custom IPS signatures. [Choosing which security features to install on the client](#)

**Table 87: Managing custom intrusion prevention signatures**

Task	Description
Create a custom library with a signature group	You must create a custom library to contain your custom signatures. When you create a custom library, you use signature groups to manage the signatures more easily. You must add at least one signature group to a custom signature library before you add the signatures. <a href="#">About custom IPS signatures</a> <a href="#">Creating a custom IPS library</a>
Add custom IPS signatures to a custom library	You add custom IPS signatures to a signature group in a custom library. <a href="#">Adding signatures to a custom IPS library</a>
Assign libraries to client groups	You assign custom libraries to client groups rather than to a location. <a href="#">Assigning multiple custom IPS libraries to a group</a>
Change the order of signatures	Intrusion prevention uses the first rule match. Symantec Endpoint Protection checks the signatures in the order that they are listed in the signatures list. <b>For example, if you add a signature group to block TCP traffic in both directions on destination port 80, you might add the following signatures:</b> <ul style="list-style-type: none"><li>• Block all traffic on port 80.</li><li>• Allow all traffic on port 80.</li></ul> If the Block all traffic signature is listed first, the Allow all traffic signature is never enacted. If the Allow all traffic signature is listed first, the Block all traffic signature is never enacted, and all HTTP traffic is always allowed. <b>Note:</b> Firewall rules take precedence over intrusion prevention signatures. <a href="#">Changing the order of custom IPS signatures</a>
Copy and paste signatures	You can copy and paste signatures between groups and between libraries.
Define variables for signatures	When you add a custom signature, you can use variables to represent changeable data in signatures. If the data changes, you can edit the variable instead of editing the signatures throughout the library. <a href="#">Defining variables for custom IPS signatures</a>
Test custom signatures	You should test the custom intrusion prevention signatures to make sure that they work. <a href="#">Testing custom IPS signatures</a>

## Creating a custom IPS library

You create a custom IPS library to contain your custom IPS signatures.

### [Managing custom intrusion prevention signatures](#)

To create a custom IPS library

1. In the console, on the **Policies** page, under **Policies**, click **Intrusion Prevention**.
2. Click the **Custom Intrusion Prevention** tab.
3. Under **Tasks**, click **Add Custom Intrusion Prevention Signatures**.
4. In the **Custom Intrusion Prevention Signatures** dialog box, type a name and optional description for the library.  
The NetBIOS Group is a sample signature group with one sample signature. You can edit the existing group or add a new group.
5. To add a new group, on the **Signatures** tab, under the **Signature Groups** list, click **Add**.
6. In the **Intrusion Prevention Signature Group** dialog box, type a group name and optional description, and then click **OK**.  
The group is enabled by default. If the signature group is enabled, all signatures within the group are enabled automatically. To retain the group for reference but to disable it, uncheck **Enable this group**.
7. Add a custom signature.

[Adding signatures to a custom IPS library](#)

## Adding signatures to a custom IPS library

You add custom intrusion prevention signatures to a new or existing custom IPS library.

### [Managing custom intrusion prevention signatures](#)

To add a custom signature

1. Create a custom IPS library.  
[Creating a custom IPS library](#)
2. On the **Signatures** tab, under **Signatures for this Group**, click **Add**.
3. In the **Add Signature** dialog box, type a name and optional description for the signature.
4. In the **Severity** drop-down list, select a severity level.  
Events that match the signature conditions are logged with this severity.
5. In the **Direction** drop-down list, specify the traffic direction that you want the signature to check.
6. In the **Content** field, type the syntax of the signature.

For example, signatures for some common protocols use the following syntax:

HTTP	<pre>rule tcp, dest=(80,443), saddr=\$LOCALHOST, msg="MP3 GET in HTTP detected", regexcontent="[Gg][Ee][Tt] .*[Mm][Pp]3 ."</pre>
FTP	<pre>rule tcp, dest=(21), tcp_flag&amp;ack, saddr=\$LOCALHOST, msg="MP3 GET in FTP detected", regexcontent="[Rr][Ee][Tt][Rr] .*[Mm][Pp]3\x0d\x0a"</pre>

For more information about the syntax, click **Help**.

[Syntax for custom intrusion prevention signatures](#)

- 
7. If you want an application to trigger the signature, click **Add**.
  8. In the **Add Application** dialog box, type the file name and an optional description for the application.  
For example, to add the application Internet Explorer, type the file name as `iexplore` or `iexplore.exe`. If you do not specify a file name, any application can trigger the signature.
  9. Click **OK**.  
The added application is enabled by default. If you want to disable the application until a later time, uncheck the check box in the **Enabled** column.
  10. In the **Action** group box, select the action you want the client to take when the signature detects the event:

Block	Identifies and blocks the event or attack and records it in the Security Log
Allow	Identifies and allows the event or attack and records it in the Security Log

11. To record the event or attack in the Packet Log, check **Write to Packet Log**.
12. Click **OK**.  
The added signature is enabled by default. If you want to disable the signature until a later time, uncheck the check box in the **Enabled** column.
13. You can add additional signatures. When you are finished, click **OK**.
14. If you are prompted, assign the custom IPS signatures to a group.  
You can also assign multiple custom IPS libraries to a group.

[Assigning multiple custom IPS libraries to a group](#)

## Changing the order of custom IPS signatures

The IPS engine for custom signatures checks the signatures in the order that they are listed in the signatures list. Only one signature is triggered per packet. When a signature matches an inbound traffic packet or outbound traffic packet, the IPS engine stops checking other signatures. So that the IPS engine executes signatures in the correct order, you can change the order of the signatures in the signatures list. If multiple signatures match, move the higher priority signatures to the top.

**For example, if you add a signature group to block TCP traffic in both directions on destination port 80, you might add the following signatures:**

- Block all traffic on port 80.
- Allow all traffic on port 80.

If the Block all traffic signature is listed first, the Allow all traffic signature is never enacted. If the Allow all traffic signature is listed first, the Block all traffic signature is never enacted, and all HTTP traffic is always allowed.

### NOTE

Firewall rules take precedence over intrusion prevention signatures.

### [Managing custom intrusion prevention signatures](#)

To change the order of custom IPS signatures

- 
1. Open a custom IPS library.
  2. On the **Signatures** tab, in the **Signatures for this Group** table, select the signature that you want to move, and then do one of the following actions:
    - To process this signature before the signature above it, click **Move Up**.
    - To process this signature after the signature below it, click **Move Down**.
  3. When you finish configuring this library, click **OK**.

## Defining variables for custom IPS signatures

When you add a custom IPS signature, you can use variables to represent changeable data in signatures. If the data changes, you can edit the variable instead of editing the signatures throughout the library.

### Managing custom intrusion prevention signatures

Before you can use the variables in the signature, you must define them. The variables that you define in the custom signature library can then be used in any signature in that library.

You can copy and paste the content from the existing sample variable to start as a basis for creating content.

1. To define variables for custom IPS signatures, create a custom IPS library.
2. In the **Custom Intrusion Prevention Signatures** dialog box, click the **Variables** tab.
3. Click **Add**.
4. In the **Add Variable** dialog box, type a name and optional description for the variable.
5. Add a content string for the variable value of up to 255 characters.

When you enter the variable content string, follow the same syntax guidelines that you use for entering values into signature content.

### Syntax for custom intrusion prevention signatures

6. Click **OK**.

After the variable is added to the table, you can use the variable in any signature in the custom library.

7. To use variables in custom IPS signatures, on the **Signatures** tab, add or edit a signature.
8. In the **Add Signature** or **Edit Signature** dialog box, in the **Content** field, type the variable name with a dollar sign (\$) in front of it.

For example, if you create a variable named HTTP for specifying HTTP ports, type the following:

```
$HTTP
```

9. Click **OK**.
10. When you finish configuring this library, click **OK**.

## Assigning multiple custom IPS libraries to a group

After you create a custom IPS library, you assign it to a group rather than an individual location. You can later assign additional custom IPS libraries to the group.

### Managing custom intrusion prevention signatures

To assign multiple custom IPS libraries to a group



1. In the console, click **Clients**.
2. Under **Clients**, select the group to which you want to assign the custom signatures.
3. On the **Policies** tab, under **Location-independent Policies and Settings**, click **Custom Intrusion Prevention**.
4. In the **Custom Intrusion Prevention for group name** dialog box, check the check box in the **Enabled** column for each custom IPS library you want to assign to that group.
5. Click **OK**.

## Testing custom IPS signatures

After you create custom IPS signatures, you should test them to make sure that they function correctly.

**Table 88: Testing custom IPS signatures**

Step	Description
Step 1: Make sure that clients use the current policy	The next time that the client receives the policy, the client applies the new custom signatures. <a href="#">Updating client policies</a>
Step 2: Test the signature content on the client	You should test the traffic that you want to block on the client computers. For example, if your custom IPS signatures should block MP3 files, try to download some MP3 files to the client computers. If the download does not occur, or times out after many tries, the custom IPS signature is successful. You can click Help for more information about the syntax that you can use in custom IPS signatures. <a href="#">Syntax for custom intrusion prevention signatures</a>
Step 3: View blocked events in Symantec Endpoint Protection Manager	You can view events in the Network and Host Exploit Mitigation Attack logs. The message you specify in the custom IPS signature appears in the log <a href="#">Monitoring endpoint protection</a>

[Managing custom intrusion prevention signatures](#)

## Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy

- [How does Memory Exploit Mitigation protect applications?](#)
- [Types of exploit protection](#)
- [Memory Exploit Mitigation requirements](#)
- [Correcting and preventing false positives](#)
- [Finding the logs and reports for Memory Exploit Mitigation events](#)
- [Auditing protection for the mitigation techniques that terminated the application](#)
- [Disabling Memory Exploit Mitigation](#)
- [Reporting false positives to Security Response](#)

### How does Memory Exploit Mitigation protect applications?

Starting in 14, Symantec Endpoint Protection includes Memory Exploit Mitigation, which uses multiple mitigation techniques to stop attacks on a vulnerability in the software. For example, when the client user runs an application such as Internet Explorer, an exploit might instead launch a different application that contains malicious code.

To stop an exploit, Memory Exploit Mitigation injects a DLL into a protected application. After Memory Exploit Mitigation detects the exploit attempt, it either blocks the exploit or terminates the application that the exploit threatens. Symantec

---

Endpoint Protection displays a notification to the user on the client computer about the detection, and logs the event in the client's Security log.

For example, the client user might see the following notification:

Symantec Endpoint Protection: Attack: Structured Exception Handler Overwrite detected. Symantec Endpoint Protection will terminate <application name> application

Memory Exploit Mitigation continues to block the exploit or terminate the application until the client computer runs a version of the software where the vulnerability is fixed.

#### **NOTE**

In 14 MPx, Memory Exploit Mitigation was called Generic Exploit Mitigation.

### **Types of exploit protection**

Memory Exploit Mitigation uses multiple types of mitigation techniques to handle the exploit, depending on which technique is most appropriate for the type of application. For example, both the StackPvt and RopHeap techniques block the exploits that attack Internet Explorer.

[Symantec Endpoint Protection Memory Exploit Mitigation techniques](#)

#### **NOTE**

If you have enabled the Microsoft App-V feature on your computers, Memory Exploit Mitigation does not protect the Microsoft Office processes that App-V protects.

### **Memory Exploit Mitigation requirements**

Memory Exploit Mitigation is only available if you have installed intrusion prevention. Memory Exploit Mitigation has its own set of separate signatures that is downloaded along with the intrusion prevention definitions. However, you can enable or disable intrusion prevention and Memory Exploit Mitigation independently.

#### **NOTE**

Starting in 14.0.1, Memory Exploit Mitigation has its own policy. In the 14 MPx releases, it is part of the Intrusion Prevention policy; if you disable the Intrusion Prevention policy on the **Overview** tab, you disable Memory Exploit Mitigation.

In addition, you must run LiveUpdate at least once for the list of applications to appear in the Memory Exploit Mitigation policy. By default, protection is enabled for all applications that appear in the policy.

[Checking that Symantec Endpoint Protection Manager has the latest content](#)

### **Correcting and preventing false positives**

Occasionally, Memory Exploit Mitigation may unintentionally terminate an application on the client computer. If you determine that an application's behavior is legitimate and was not exploited, the detection is a false positive. For false positives, you should disable protection until Symantec Security Response changes the Memory Exploit Mitigation behavior.

The following table displays the steps to handle false positive detections.

**Table 89: Steps to find and remediate a false positive**

Tasks	
Step 1: Find out which applications terminate unexpectedly on the client computers.	<p>You can find out which applications were terminated on the client computer in the following ways:</p> <ul style="list-style-type: none"> <li>A user on the client computer notifies you that an application does not run.</li> <li>Open the Memory Exploit Mitigation log or report that lists which mitigation technique terminated the applications on the client computer.</li> </ul> <p><b>Note:</b> Sometimes the mitigation techniques do not produce logs due to the nature of the exploit.</p> <p><a href="#">Finding the logs and reports for Memory Exploit Mitigation events</a></p>
Step 2: Disable protection and audit the techniques that terminate the application.	<p>Disable protection at the most minimal level first so that other processes remain protected. Do not turn off Memory Exploit Mitigation to allow the application to run until you have tried all other methods. After each of the following subtasks, go to Step 3.</p> <ol style="list-style-type: none"> <li>First, audit the protection for the specific application that the mitigation technique terminated. For example, if Mozilla Firefox was terminated, you would disable either the SEHOP technique or the HeapSpray technique. Sometimes a mitigation technique does not create log events due to the nature of the exploit, so you cannot be sure which mitigation technique terminated the application. In this case, you should disable each technique that protects that application, one at a time, until you find which technique caused the termination.</li> <li>Audit protection for all applications that a single mitigation technique protects.</li> <li>Audit protection for all applications, regardless of the technique. This option is similar to disabling Memory Exploit Mitigation, except that the management server collects the log events for detections. Use this option to check for false positives on legacy 14 MPx clients.</li> </ol> <p><a href="#">Auditing protection for the mitigation techniques that terminated the application</a></p>
Step 3: Update the policy on the client computer, and rerun the application.	<ul style="list-style-type: none"> <li>If the application runs correctly, the detection for that mitigation technique is a false positive.</li> <li>If the application does not run the way you expect it to, the detection is a true positive.</li> <li>If the application still terminates, audit at a level restrictive level. For example, audit a different mitigation technique or for all applications that the technique protects.</li> </ul> <p><a href="#">Updating client policies</a></p>
Step 4: Report the false positives and reenable protection for the true positives.	<p>For false positive detections:</p> <ol style="list-style-type: none"> <li>Notify the Symantec team that the detection was a false positive. See <a href="#">Symantec Insider Tip: Successful Submissions!</a></li> <li>Keep protection disabled for the terminated application by setting each technique's action to <b>No</b>.</li> <li>After Security Response resolves the issue, reenable protection by changing the technique's action to <b>Yes</b>.</li> </ol> <p>For true positive detections:</p> <ol style="list-style-type: none"> <li>Reenable protection by changing the rule's action for that mitigation technique back to <b>Yes</b>.</li> <li>Check whether there is a patched version or a newer release of the infected application that fixes the current vulnerability. After you install the patched application, rerun it on the client computer to see if Memory Exploit Mitigation still terminates the application.</li> </ol>

### Finding the logs and reports for Memory Exploit Mitigation events

You need to view the logs and run quick reports to find the applications that Memory Exploit Mitigation terminated.

1. In the console, do one of the following actions:

- For logs, click **Monitors > Logs > Network and Host Exploit Mitigation** log type > **Memory Exploit Mitigation** log content > **View Log**.

Look for the **Memory Exploit Mitigation Blocked Event** event type. The **Event type** column lists the mitigation technique, and the **Action** column lists whether or not the application in the **Application Name** column was blocked. For example, the following log event indicates a Stack Pivot attack:

Attack: Return Oriented Programming Changes Stack Pointer

- 
- For quick reports, click **Reports > Quick Reports > Network and Host Exploit Mitigation** report type > **Memory Exploit Mitigation Detections** report > **Create Report**.

Look for the blocked Memory Exploit Mitigation detections.

### Auditing protection for a terminated application

When you test for false positives, change the Memory Exploit Mitigation behavior so that it audits a detection, but lets the application run. However, Memory Exploit Mitigation does not protect the application.

To audit protection for a terminated application

2. In the console, click **Policies > Memory Exploit Mitigation > Memory Exploit Mitigation**.
3. On the **Mitigation Techniques** tab, next to **Choose a mitigation technique**, select the technique that terminated the application, such as **StackPvt**.
4. Under the **Protected** column, select the terminated application, and then change **Default (Yes)** to **Log Only**.

Change the action to **No** after you verified that the detection is a true false positive. Both **Log Only** and **No** allow the possible exploit, but also let the application run.

Some applications have multiple mitigation techniques that block the exploit, so follow this step for each technique individually.

5. (Optional) Do one of the following steps, and then click **OK**:
  - If you are not sure which technique terminated the application, click **Choose a protection action for all applications for this technique**. This option overrides the settings for each technique.
  - If you have a mix of 14.0.1 clients and legacy 14 MPx clients, and you only want to test the 14.0.1 clients, click **Set the protection action for all techniques to log only**.
6. (Optional) To test the application regardless of technique, on the **Application Rules** tab, in the **Protected** column, uncheck the terminated application, and then click **OK**.

For legacy 14 MPx clients, you can only use this option. After you upgrade to version 14.0.1 clients, reenables protection and do the finer grained tuning. Open the **Computer Status** log to find which clients run which product version.

7. In the console, click **Policies > Memory Exploit Mitigation**.
8. Uncheck **Enable Memory Exploit Mitigation**.
9. Click **OK**.
10. In the Symantec Endpoint Protection Manager, make sure that Symantec Insight is enabled. Insight is enabled by default.

### [Customizing Download Insight settings](#)

11. Download and run the SymDiag tool on the client computer. See: [Download SymDiag to detect product issues](#)
12. On the SymDiag tool **Home** page, click **Collect Data for Support**, and for the **Debug logging > Advanced** option, set the **WPP Debug > Trace Level** to **Verbose**.

### [Advanced debug log options in SymDiag for Endpoint Protection clients](#)

- 
13. Reproduce the false positive detection.
  14. After the log collection finishes, submit the .sdbz file to <https://mysymantec.force.com/customer/s/> by opening a new case or updating an existing case with this new information.
  15. Submit the detected application to the [SymSubmit site](#), and do the following tasks:
    - Choose when the detection occurred, choose the **B2 Symantec Endpoint Protection 14.x** product, and click the **C5 - IPS** event.
    - In the submission notes, provide the Technical Support case number from the previous step, the application that triggered the MEM detection, and details about the application's version number.  
For example, you might add: "Blocked Attack: Return Oriented Programming API Invocation attack against C:\Program Files\VideoLAN\VLC\vlc.exe", the version for vlc.exe is 2.2.0-git-20131212-0038. This is not the latest available version but it is the version that our organization is required to use."  
[Symantec Insider Tip: Successful Submissions!](#)
  16. On the client computer, compress a copy of the submissions folder that is located at: %PROGRAMDATA%\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\CmnClnt\ccSubSDK.  
  
Submit this folder to Technical Support and notify them of the tracking number for the false positive submission that you opened in the previous step. Technical Support ensures that all necessary logs and materials are intact and associated with the false positive investigation.

## Symantec Endpoint Protection Memory Exploit Mitigation techniques

Starting in version 14, Memory Exploit Mitigation (MEM) stops vulnerability attacks on software on your Windows client computers. MEM uses the following types of mitigation techniques to stop these attacks:

- **SEHOP** (Structured exception handling overwrite protection) (14)  
Memory Exploit Mitigation provides structured exception handling overwrite protection for applications such as the RealPlayer media player. An exploit attack can control the execution flow of software toward the attacker's shellcode by using an overwrite exception handler function. The exception handler function address is stored in stack memory and can easily be overwritten when a stack buffer overflow exists. Windows operating systems include SEHOP, but some Windows Vista operating systems disable SEHOP by default. Memory Exploit Mitigation provides protection even if SEHOP in Windows is turned off. SEHOP attacks occur on 32-bit clients only.
- **Java Security Manager** (14)  
Memory Exploit Mitigation blocks Java Applets that try to disable Windows Security Manager. Some exploit attacks use a Java Applet to turn off Security Manager to allow Java code to execute privileged actions.
- **StackPvt (StackPivot)** (14.0.1)  
The Stack Pivot technique detects if the call stack address changed. This event indicates the exploit changed the stack pointer (ESP) register to point to the exploit's fake or crafted call stack memory. The fake memory contains the ROP attack chains.
- **ForceDEP** (Force Data Execution Prevention) (14.0.1)  
Exploit attacks usually insert their malicious executable code (called shellcode) into the stack memory (using the buffer overflow) or heap memory (using heap spraying). The exploit then hijacks the flow of execution towards these locations. To mitigate this attack, Windows XP SP2 and later includes data execution prevention (DEP), a system-level protection that marks these memory locations as non-executable. However, the problem is that this feature can be turned off using a `SetProcessDEPPolicy()` API call. Additionally, for a process to be protected with DEP, it should be compiled with the `/NXCOMPAT` switch. The **ForceDEP** technique prevents DEP from being turned off, even on those programs that are not compiled with that switch.
- **ForceASLR** (Force address space layout randomization) (14.0.1)  
For an exploit to modify or damage the operating system, it needs to call system APIs, such as `URLDownloadToFile` and `CreateProcess`. In early Windows XP and earlier, system DLLs such as `Kernel32.dll` were always loaded to fixed and predictable memory locations. Therefore, hard-coded addresses easily called APIs. Additionally, after

---

DEP was introduced, exploits have invented alternative method to execute code called return-oriented programming (ROP). Rather than write and execute shellcode in stack or heap memory, the shellcode is instead constructed using a combination of existing executable code bytes from various DLLs loaded in the process. To prevent this process, Windows Vista and later versions introduced ASLR. This feature randomizes the load address of DLLs in the memory, which makes hard-coded address use ineffective. However, for a DLL to be loaded in random memory it should have been compiled with `/DYNAMICBASE` switch. Some old DLLs are still compiled without this switch, which exploits can take advantage of. ForceASLR makes the ASLR mandatory on those DLLs.

- **HeapSpray (14)**

A heap spray attack occurs when the attacker tries to place its attack code to a predetermined memory location. The HeapSpray technique reserves the commonly used memory locations to prevent an attacker from using them. Heap spray attacks are a type of buffer attack that is seen in older web browsers and applications.

- **EnhASLR (Enhance Address space layout randomization) (14.0.1)**

The EnhASLR technique allocates random memory regions in a process. The allocation of memory becomes less predictable, which helps to mitigate heap spraying. EnhASLR also increases entropy for ASLR and DLL relocations.

- **NullProt (Null Page Protection) (14.0.1)**

NULL (0x00000000) is a valid memory address that an exploit may take advantage of. The NullProt technique pre-allocates this memory location to avoid its potential use.

- **DIILoad (14.0.1)**

Prevents a process from loading a DLL from a shared folder. Some exploits use this vector to execute DLL directly from their malicious servers, such as `\\malicious.com\malware.dll`. Note that the DIILoad technique does not prevent remote loading of DLL's over local networks such as the localhost, link local, and private IP addresses. Between the time the load path is checked and the actual loading, the result of querying the DNS server for a remote path with a host name might be different.

The following mitigation techniques protect against return-oriented programming (ROP) attacks:

- **StackNX (14.0.1)**

The StackNX technique prevents call to memory protection APIs such as `VirtualProtect` to mark the memory addresses that belong to the stack as an executable.

- **RopCall (14.0.1)**

Ensures that system critical APIs are called from the call instructions and not from the existing RET instructions or jump instructions.

- **RopHeap (14.0.1)**

Denies the calls to memory protection APIs to the heap that is then executed using the return instruction.

- **RopFlow**

The RopFlow technique performs a simulation of execution of return addresses in the call stack when a system critical API is called. RopFlow checks whether the RET instruction points to either another critical API or to memory that is not properly marked as executable. Either event indicates that an ROP attack occurred. RopFlow simulates a maximum allowed number of instructions to avoid a performance impact.

Memory Exploit Mitigation events are logged in to the Security log on the client and in the Memory Exploit Mitigation log on Symantec Endpoint Protection Manager. These events are similar to IPS events except that the event IDs use the signature ID range of 61000-61999.

#### **NOTE**

If you have installed or enabled the following applications on the client computers, MEM does not protect the processes that these applications protect:

Windows Enhanced Mitigation Experience Toolkit (EMET)

Microsoft Application Virtualization (App-V) feature

[Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy](#)

---

# Ransomware mitigation and protection with Symantec Endpoint Protection

## What is ransomware?

Ransomware is a category of malware that encrypts documents, which makes them unusable, and leaves the rest of the computer accessible. Ransomware attackers try to force their victims to pay a ransom through specifically noted payment methods after which they may or may not grant the victims access to their data.

Targeted ransomware is more complex than the original ransomware attacks and involves more than just the initial infection. Attackers have found more ways of extorting victim organizations using the following range of distribution methods:

- **Phishing:** Emails sent to employees disguised as work-related correspondence.
- **Malvertising:** Compromising media websites in order to serve malicious ads containing a JavaScript-based framework known as SocGholish which masquerades as a software update.
- **Vulnerability exploitation:** Exploiting vulnerable software running on public-facing servers.
- **Secondary infections:** Leveraging pre-existing botnets in order to gain a foothold on the victim's network.
- **Poorly secured services:** Attacking organizations through poorly secured RDP services, taking advantage of leaked or weak credentials.

## Protecting against ransomware with Symantec Endpoint Protection

Most of the features to protect against ransomware in Symantec Endpoint Protection, are enabled by default. For more information on which features protect your environment, see:

[Ransomware protection using Symantec Endpoint Protection](#)

[Protecting against ransomware with Symantec Endpoint Security](#)

## Best practices to mitigate ransomware

Hardening Your Environment Against Ransomware



In addition to enabling SEP protection, to avoid ransomware infection, follow these steps.

Step	Action
<b>1. Protect your local environment</b>	<ol style="list-style-type: none"><li>1. <b>Ensure you have the latest version of PowerShell</b> and that you have logging enabled.</li><li>2. <b>Restrict access to RDP services.</b> Only allow RDP from specific known IP addresses, and ensure you are using multi-factor authentication. Use File Server Resource Manager (FSRM) to lock out the ability to write known ransomware extensions on file shares where user write access is required.</li><li>3. <b>Create a plan to consider notification of outside parties.</b> In order to ensure correct notification of required organizations, such as the FBI or other law enforcement authorities/agencies, be sure to have a plan in place to verify.</li><li>4. <b>Create a “jump bag” with hard copies and archived soft copies of all critical administrative information.</b> In order to protect against the compromise of the availability of this critical information, store it in a jump bag with hardware and software needed to troubleshoot problems. Storing this information on the network is not helpful when network files are encrypted. Implement proper audit and control of administrative account usage. You could also implement one-time credentials for administrative work to help prevent theft and usage of admin credentials.</li><li>5. <b>Create profiles of usage for admin tools.</b> Many of these tools are used by attackers to move laterally undetected through a network. A user account that has a history of running as admin using PsInfo/PsExec on a small number of systems is probably fine, but a service account running PsInfo/PsExec on all systems is suspicious.</li></ol>
<b>2. Protect your email system</b>	<ol style="list-style-type: none"><li>1. Enable two-factor authentication (2FA) to prevent compromise of credentials during phishing attacks.</li><li>2. <b>Harden security architecture around email systems</b> to minimize the amount of spam that reaches end-user inboxes and ensure you are following best practices for your email system, including the use of SPF and other defensive measures against phishing attacks.</li></ol>
<b>3. Make backups</b>	<p>Regularly back up the files on both the clients and servers. Either back up the files when the computers are offline or use a system that networked computers and servers cannot write to. If you do not have dedicated backup software, you can also copy the important files to removable media. Then eject and unplug the removable media; do not leave the removable media plugged in.</p> <ol style="list-style-type: none"><li>1. <b>Implement offsite storage of backup copies.</b> Arrange for offsite storage of at least four weeks of weekly full and daily incremental backups.</li><li>2. <b>Implement offline backups that are onsite.</b> Make sure you have backups that are not connected to the network to prevent them from being encrypted by ransomware. Removal is best done with the system off the networks to prevent any potential spread of the threat.</li><li>3. <b>Verify and test your server-level backup solution.</b> This should already be part of your disaster recovery process.</li><li>4. <b>Secure the file-level permissions for backups and backup databases.</b> Don't let your backups get encrypted.</li><li>5. <b>Test restore capability.</b> Ensure restore capabilities support the needs of the business. Lock down mapped network drives by securing them with a password and access control restrictions. Use read-only access for files on network drives, unless it is absolutely necessary to have write access for these files. Restricting user permissions limits which files the threats can encrypt.</li></ol>

### What should you do if you get ransomware?

There is no ransomware removal tool. No security product can decrypt files that ransomware encrypts. Instead, if your client computers do get infected with ransomware and your data is encrypted, follow these steps:

#### 1. **Do not pay the ransom.**

If you pay the ransom:



- There is no guarantee that the attacker will supply a method to unlock your computer or decrypt your files.
  - The attacker uses the ransom money to fund additional attacks against other users.
2. **Isolate the infected computer before the ransomware can attack network drives to which it has access.**
  3. **Use Symantec Endpoint Protection Manager or SES to update the virus definitions and scan the client computers.**

New definitions are likely to detect and remediate the ransomware. Symantec Endpoint Protection Manager automatically downloads virus definitions to the client, as long as the client is managed and connected to the management server or cloud console.

    - In Symantec Endpoint Protection Manager, click **Clients**, right-click the group, and click **Run a command on the group > Update Content and Scan**.
    - In Symantec Endpoint Security, run the **Scan Now** command. See: [Running commands on client devices](#)
  4. **Reinstall using a clean installation.**

If you restore encrypted files from a backup, you can get your restored data but it's possible that other malware was installed during the course of the attack.
  5. **Submit the malware to Symantec Security Response.**

If you can identify the malicious email or executable, submit it to Symantec Security Response. These samples enable Symantec to create new signatures and improve defenses against ransomware. See: [Symantec Insider Tip: Successful Submissions!](#)

## Ransomware protection using Symantec Endpoint Protection

Targeted ransomware attacks can be broken down into the following broad phases:

- Initial compromise
- Privilege escalation and credential theft
- Lateral movement
- Encryption and deletion of backups

The best defense is to block the many types of attacks and know the attack chain that most cyber crime groups use to identify security priorities. Unfortunately, ransomware decryption is not possible using removal tools.

On Symantec Endpoint Protection Manager, deploy and enable the following features. Some features are enabled by default.

**Table 90: Symantec Endpoint Protection Manager features**

Step	Action
<b>Step 1: Enable file-based protection</b> Symantec quarantines the following types of files: Ransom.Maze, Ransom.Sodinokibi, and Backdoor.Cobalt	Enable the Virus and Spyware Protection policy, which is enabled by default. <a href="#">Preventing and handling virus and spyware attacks on client computers</a>
<b>Step 2: Enable SONAR</b> SONAR's behavioral-based protection is another crucial defense against malware. SONAR prevents the double executable file names of ransomware variants like CryptoLocker from running.	In a Virus and Spyware Protection policy, click <b>SONAR &gt; Enable SONAR</b> . This option is enabled by default. See: <a href="#">Managing SONAR</a>

<p><b>Step 3: Modify Download Insight</b></p> <p>Symantec Insight prevents ransomware variants by quarantining the files that the Symantec customer base knows are malicious or that haven't yet been proven to be either safe or malicious.</p>	<p>Download Insight is part of the default <b>Virus and Spyware - High Security</b> policy.</p> <ol style="list-style-type: none"> <li>1. In the console, open the target Virus and Spyware Protection policy and click <b>Download Protection</b>. If adding a new policy, select the <b>Virus and Spyware Protection policy - High Security</b> policy.</li> <li>2. On the <b>Download Insight</b> tab, make sure that <b>Enable Download Insight to detect potential risks in downloaded files based on file reputation</b> is checked.</li> <li>3. Check the following default options: <ul style="list-style-type: none"> <li>— <b>Files with 5 or fewer users</b></li> <li>— <b>Files known by users for 2 or fewer days</b></li> </ul> <p>The low default values force the client to treat any file that has not been reported to Symantec by more than five users or for less than 2 days to be treated as unproven files. When unproven files meet these criteria, Download Insight detects the files as malicious.</p> </li> <li>4. Make sure that <b>Automatically trust any file downloaded from a trusted Internet or intranet site</b> is checked.</li> <li>5. On the <b>Actions</b> tab, under <b>Malicious Files</b>, keep the first action as <b>Quarantine risk</b> and the second action as <b>Leave alone</b>.</li> <li>6. Under <b>Unproven Files</b>, click <b>Quarantine risk</b>.</li> <li>7. Click <b>OK</b>.</li> </ol>
<p><b>Step 4: Enable the Intrusion Prevention System (IPS)</b></p> <ul style="list-style-type: none"> <li>• IPS blocks some threats that traditional virus definitions alone cannot stop. IPS is the best defense against drive-by downloads, which occurs when software is unintentionally downloaded from the Internet. Attackers often use exploit kits to deliver a web-based attack like CryptoLocker through a drive-by download.</li> <li>• In some cases, IPS can block file encryption by interrupting command-and-control (C&amp;C) communication. A C&amp;C server is a computer controlled by an attacker or cybercriminal and that is used to send commands to systems compromised by malware and receive stolen data from a target network.</li> <li>• <b>URL reputation</b> prevents web threats based on the reputation score of a web page. The <b>Enable URL Reputation</b> option blocks web pages with reputation scores below a specific threshold. (14.3 RU1 and later).</li> </ul>	<p>For more information, see:  <a href="#">Enabling network intrusion prevention or browser intrusion prevention</a>  URL reputation is enabled by default.</p>
<p><b>Step 5: Block PDF files and scripts</b></p>	<p>In the Exceptions policy, click <b>Windows Exceptions &gt; File Access</b>.</p>

<p><b>Step 6: Download patches</b></p> <p>Download the latest patches for web application frameworks, web browsers, and web browser plug-ins.</p>	<p>Do the following:</p> <ol style="list-style-type: none"> <li>1. Use the Application and Device Control to prevent applications from running in the User Profile directories, such as Local and LocalLow. Ransomware applications install themselves into many directories apart from Local\Temp\Low. See: <a href="#">Strengthening anti-virus security to prevent Ransomware derivative (Trojan.Cryptolocker family, etc.) infections</a></li> <li>2. Use Endpoint Detection Response (EDR) to identify files with ransomware behavior: <ol style="list-style-type: none"> <li>a. Disable macro scripts from MS Office files that are transmitted through email.</li> <li>b. Right-click the detected endpoints and select <b>Isolate</b>. To isolate and rejoin endpoints from the console, you must have a Quarantine Firewall policy in Symantec Endpoint Protection Manager that is assigned to a Host Integrity policy. See: <a href="#">About Host Integrity and Quarantine Firewall Policies</a></li> </ol> </li> </ol>
<p><b>Step 7: Enable Web and Cloud Access Protection and Web Security Service</b></p> <p>Use Web and Cloud Access Protection and secure connection settings so that whether on a corporate network, at home or out of office, endpoints have the ability to integrate with Symantec Web Security Service (WSS). NTR redirects Internet traffic on the client to the Symantec WSS, where the traffic is allowed or blocked based on the WSS policies.</p>	<p>For more information, see: <a href="#">Configuring Web and Cloud Access Protection</a></p>
<p><b>Step 8: Enable Memory Exploit Mitigation</b></p> <p>Protects against known vulnerabilities in unpatched software, such as JBoss or Apache web server, which attackers exploit.</p>	<p>For more information, see: <a href="#">Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy</a></p>
<p><b>Step 9: Enable AMSI and file-less scanning</b></p> <p>Third-party application developers can protect their customers from dynamic script-based malware and from non-traditional avenues of cyberattack. The third-party application calls the Windows AMSI interface to request a scan of user-provided script, which is routed to the Symantec Endpoint Protection client. The client responds with a verdict to indicate on whether or not the script behavior is malicious. If the behavior is not malicious, then the script execution proceeds. If the script's behavior is malicious, the application does not run it. On the client, the Detection Results dialog box displays a status of "Access Denied." Examples of third-party scripts include Windows PowerShell, JavaScript, and VBScript. Auto-Protect must be enabled. This functionality works for Windows 10 and later computers.</p> <p>14.3 and later.</p>	<p>Enabled by default. See: <a href="#">How the Antimalware Scan Interface (AMSI) helps you defend against malware</a> <a href="#">Antimalware Scan Interface (AMSI)</a></p>

<b>Step 10: Enable Endpoint Detection and Response (EDR)</b> EDR focuses on behaviors rather than files and can strengthen defenses against spear phishing and use of living-off-the-land tools. For example, if Word doesn't normally launch PowerShell in the customer environment, then this should be placed in Block mode. EDR's UI allows customers to easily understand which behaviors are common and should be allowed, which are seen but should still be alerted on, and which are uncommon and should be blocked. You can also address gaps reactively as part of investigating and responding to incident alerts. The incident alert will show all behaviors that were observed as part of the breach and provides the capability to put this in block mode right from the incident details page.	For more information, see: <a href="#">Configuring client groups to use private servers for reputation queries and submissions</a>
<b>Step 11: Enable auditing</b> Use auditing tools to help you gain insight into your endpoints both on a corporate network and outside of your corporate network before ransomware has a chance to spread.	Use Memory Exploit Mitigation to test for false positives. See: <a href="#">Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy</a>
<b>Step 12: Set up unmanaged detectors</b> Unmanaged detectors need to be present to account for endpoints where protection may not be present.	<a href="#">Configuring a client to detect unmanaged devices</a>

[Ransomware removal and protection with Symantec Endpoint Protection](#)

## Preventing and handling virus and spyware attacks on client computers

You can prevent and handle virus and spyware attacks on client computers by following some important guidelines.

**Table 91: Protecting computers from virus and spyware attacks**

Task	Description
Make sure that your computers have Symantec Endpoint Protection installed	All computers in your network and all your servers should have Symantec Endpoint Protection installed. Make sure that Symantec Endpoint Protection is functioning correctly. <a href="#">Viewing the protection status of client computers</a>
Keep definitions current	Make sure that the latest definitions are installed on client computers. You can check the definitions date on the <b>Clients</b> tab. You can run a command to update the definitions that are out of date. You can also run a computer status report to check the latest definitions date. <a href="#">How to update content and definitions on the clients</a>

Task	Description
Run regular scans	<p>By default, Auto-Protect and SONAR run on client computers. A default scheduled active scan also runs on client computers.</p> <p>You can run scans on demand. You can customize the scan settings.</p> <p><a href="#">Running on-demand scans on client computers</a></p> <p>You might want to create and customize scheduled scans.</p> <p>Typically, you might want to create a full scheduled scan to run once a week, and an active scan to run once per day. By default, Symantec Endpoint Protection generates an active scan that runs at 12:30 P.M. On unmanaged computers, Symantec Endpoint Protection also includes a default startup scan that is disabled.</p> <p>You should make sure that you run an active scan every day on the computers in your network. You might want to schedule a full scan once a week or once a month if you suspect that you have an inactive threat in your network. Full scans consume more computer resources and might affect computer performance.</p> <p><a href="#">Setting up scheduled scans that run on Windows computers</a></p> <p><a href="#">Setting up scheduled scans that run on Mac computers</a></p> <p><a href="#">Setting up scheduled scans that run on Linux computers</a></p>
Let clients upload critical events immediately	<p>Make sure that clients (Windows only) can bypass the heartbeat interval and send critical events to the management server immediately. Critical events include any risk found (except cookies) and any intrusion event. You can find this option in <b>Clients &gt; Policies &gt; Communications Settings</b>. The option is enabled by default.</p> <p>Administrator notifications can alert you right away when the damper period for relevant notifications is set to <b>None</b>.</p> <p><a href="#">Setting up administrator notifications</a></p> <p><b>Note:</b></p>
Check or modify scan settings for increased protection	<p>By default, virus and spyware scans detect, remove, and repair the side effects of viruses and security risks.</p> <p>The default scan settings optimize your client computers' performance while still providing a high level of protection. You can increase the level of protection, however.</p> <p>For example, you might want to increase the Bloodhound heuristic protection.</p> <p>You also might want to enable scans of network drives.</p> <p><a href="#">Adjusting scans to increase protection on your client computers</a></p>
Allow clients to submit information about detections to Symantec	<p>Clients can submit information about detections to Symantec. The submitted information helps Symantec address threats.</p> <p><a href="#">Understanding server data collection and client submissions and their importance to the security of your network</a></p>
Run intrusion prevention	<p>Symantec recommends that you run intrusion prevention on your client computers as well as Virus and Spyware Protection.</p> <p><a href="#">Managing intrusion prevention</a></p>
Remediate infections if necessary	<p>After scans run, client computers might still have infections. For example, a new threat might not have a signature, or Symantec Endpoint Protection was not able to completely remove the threat. In some cases, client computers require a restart for Symantec Endpoint Protection to complete the cleaning process.</p> <p><a href="#">Removing viruses and security risks</a></p>

## Removing viruses and security risks

You remediate risks as part of handling virus and spyware attacks on your computers.

You use the Reports and Monitors features in the console to determine what computers are infected and to view the results of remediation.

**Table 92: Removing viruses and security risks**

Step	Description
Step 1: Identify infected and at-risk computers	<p>You can get information about infected and at-risk computers from Symantec Endpoint Protection Manager. On the Home page, check the Newly Infected and the Still Infected counts in the Virus and Risks Activity Summary. The Newly Infected count is a subset of the Still Infected count. The Newly Infected count shows the number of infected and at-risk computers during the time interval that you specify in the summary.</p> <p><b>Note:</b> Unremediated SONAR detections are not counted as Still Infected. They are part of the Suspicious count in the summary.</p> <p>Computers are considered still infected if a subsequent scan detects them as infected. For example, a scheduled scan might partially clean a file. Auto-Protect subsequently detects the file as a risk.</p> <p>Files that are considered "still infected" are rescanned when new definitions arrive or as soon as the client computer is idle.</p> <p><a href="#">Identifying the infected and at-risk computers</a></p>
Step 2: Update definitions and rescan	<p>You should make sure that clients use the latest definitions.</p> <p>For legacy clients that run on Windows computers, you should also make sure that your scheduled and on-demand scans use the Insight Lookup feature. As of 14, scheduled and on-demand scans always use Insight Lookup.</p> <p>You can check the definitions date in the Infected and At Risk Computers report. You can run the Update Content and Scan command from the Risk log.</p> <p>When the Virus and Risks Activity Summary on the Home page shows the Still Infected and the Newly Infected counts are zero, then all risks are eliminated.</p> <p><a href="#">How to update content and definitions on the clients</a></p>
Step 3: Check scan actions and rescan	<p>Scans might be configured to leave the risk alone. You might want to edit the Virus and Spyware Protection policy and change the action for the risk category. The next time the scan runs, Symantec Endpoint Protection applies the new action.</p> <p>You set the action on the <b>Actions</b> tab for the particular scan type (administrator-defined or on-demand scan, or Auto-Protect). You can also change the detection action for Download Insight and SONAR.</p> <p><a href="#">Checking the scan action and rescanning the identified computers</a></p>
Step 4: Restart computers if necessary to complete remediation	<p>Computers may still be at risk or infected because they need to be restarted to finish the remediation of a virus or security risk.</p> <p>You can view the Risk log to determine if any computers require a restart.</p> <p>You can run a command from the Computer Status log to restart computers.</p> <p><a href="#">Running commands on client computers from the console</a></p>
Step 5: Investigate and clean remaining risks	<p>If any risks remain, you should investigate them further.</p> <p>You can check the Symantec Security Response webpage for up-to-date information about viruses and security risks.</p> <p><a href="http://securityresponse.symantec.com">http://securityresponse.symantec.com</a></p> <p>On the client computer, you can also access the Security Response website from the scan results dialog box.</p> <p>You can also run Power Eraser from Symantec Endpoint Protection Manager to analyze and remediate difficult, persistent threats. Power Eraser is an aggressive analysis that you should run on one computer or a small number of computers only when the computers are unstable or heavily infected.</p> <p><a href="#">What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console</a></p> <p>Symantec Technical Support also offers a Threat Expert tool that quickly provides detailed analysis of threats. You can also run a load point analysis tool that can help you troubleshoot problems. You run these tools directly on the client computer.</p> <p><a href="#">Troubleshooting computer issues with the Symantec Diagnostic Tool (SymDiag)</a></p>

Step	Description
Step 6: Check the Computer Status log	View the Computer Status log to make sure that risks are remediated or removed from client computers. <a href="#">Viewing logs</a>

For more information, see [Virus removal and troubleshooting on a network](#).

[Preventing and handling virus and spyware attacks on client computers](#)

[Monitoring endpoint protection](#)

## Identifying the infected and at-risk computers

You can use the Symantec Endpoint Protection Manager Home page and a Risk report to identify the computers that are infected and at risk.

To identify infected computers

1. In the console, click **Home** and view the Virus and Risks Activity Summary.

If you are a system administrator, you see counts of the number of Newly Infected and Still infected computers in your site. If you are a domain administrator, you see counts of the number of Newly Infected and Still infected computers in your domain.

Still Infected is a subset of Newly Infected, and the Still Infected count goes down as you eliminate the risks from your network. Computers are still infected if a subsequent scan would report them as infected. For example, Symantec Endpoint Protection might have been able to clean a risk only partially from a computer, so Auto-Protect still detects the risk.

2. In the console, click **Reports**.
3. In the **Report type** list box, click **Risk**.
4. In the **Select a report** list box, click **Infected and At Risk Computers**.
5. Click **Create Report** and note the lists of the infected and at-risk computers that appear.

[Removing viruses and security risks](#)

## Checking the scan action and rescanning the identified computers

If you have infected and at-risk computers, you should identify why the computers are still infected or at risk. Check the action that was taken for each risk on the infected and at-risk computers. It may be that the action that was configured and taken was Left Alone. If the action was Left Alone, you should either clean the risk from the computer, remove the computer from the network, or accept the risk. For Windows clients, you might want to edit the Virus and Spyware Protection policy and change the scan action.

[Removing viruses and security risks](#)

To identify the actions that need to be changed and rescan the identified computers

1. In the console, click **Monitors**.
2. On the **Logs** tab, select the Risk log, and then click **View Log**.

From the Risk log event column, you can see what happened and the action that was taken. From the Risk Name column, you can see the names of the risks that are still active. From the Domain Group User column you can see which group the computer is a member of.

---

If a client is at risk because a scan took the action **Left Alone**, you may need to change the Virus and Spyware Protection policy for the group. In the **Computer** column, you can see the names of the computers that still have active risks on them.

[Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)

If your policy is configured to use push mode, it is pushed out to the clients in the group at the next heartbeat.

[Updating policies and content on the client using push mode or pull mode](#)

3. Click **Back**.
4. On the **Logs** tab, select the Computer Status log, and then click **View Log**.
5. If you changed an action and pushed out a new policy, select the computers that need to be rescanned with the new settings.
6. In the **Command** list box, select **Scan**, and then click **Start** to rescan the computers.

You can monitor the status of the Scan command from the **Command Status** tab.

## How Windows clients receive definitions from the cloud

In 14 and later, Symantec Endpoint Protection standard and embedded/VDI clients provide real-time protection with definitions in the cloud. Earlier versions provided some cloud protection with various features, such as Download Insight. Now, all virus and spyware features use the cloud to evaluate files. Cloud content includes the entire set of virus and spyware definitions as well as the latest information that Symantec has about files and potential threats.

### NOTE

The Intelligent Threat Cloud Service is supported on Windows clients only.

### Clients support cloud-enabled content

Cloud-enabled content includes a reduced-sized set of definitions that provides full protection. When the client requires new definitions, the client downloads or looks up the definitions in the cloud for better performance and speed.

Your client type must support cloud-enabled content.

You can see your client type in **Help > Troubleshooting > Install Settings**.

Standard clients and embedded/VDI clients support cloud-enabled content.

### All scans automatically use cloud lookups

**Cloud lookups include queries to Symantec Insight for file reputation information and definition checking in the cloud.**

- Scheduled and on-demand scans automatically perform cloud lookups.
- Auto-Protect also automatically performs cloud lookups. Auto-Protect now runs in user mode rather than kernel mode to reduce memory usage and provide better performance.

In addition to leveraging a smaller footprint with definitions on disk, the Intelligent Threat Cloud Service provides a 15-percent reduction in scan time.

Clients automatically send information about file reputation lookups to Symantec.

### How cloud lookups work in your network

Symantec Endpoint Protection sends cloud lookups directly to the cloud.

If you want to use a proxy server, you can specify an HTTPS proxy in the client's browser Internet options. Or you can use the Symantec Endpoint Protection Manager console to specify the HTTPS proxy for clients in **Policies > External Communications**.



---

The amount of bandwidth that the Intelligent Threat Cloud Service clients use is nearly identical to pre-14 clients, which use reputation lookups only with specific features such as Download Insight.

### **How Symantec Endpoint Protection Manager alerts you about cloud lookup errors**

If clients try cloud lookups for 3 days without success, by default Symantec Endpoint Protection Manager sends an email notification to system administrators. You can also view the alert in **Monitors > Logs > System Logs > Client Activity**. The notification condition type is **File Reputation Detection**.

### **What are portal files?**

Download Insight marks a file as a portal file when it examines a file that a user downloads from a supported portal. Scheduled and on-demand scans, Auto-Protect, and Download Insight evaluate the reputation of portal files using the sensitivity level that is set for Download Insight.

#### **NOTE**

Download Insight must be enabled to mark files as portal files.

Supported portals include: Internet Explorer, Firefox, Microsoft Outlook, Outlook Express, Google Chrome, Windows Live Messenger, and Yahoo Messenger. The portal list (or Auto-Protect portal list) is part of the Virus and Spyware Protection content that LiveUpdate downloads to the management server or the client.

Scans and Download Insight always evaluate non-portal files with a default internal sensitivity level that Symantec sets. The internal default detects only the most malicious files.

### **An example of cloud lookups in action**

An example of the way the Intelligent Threat Cloud Service protects clients:

- The client user runs Internet Explorer and tries to download a file. Download Insight uses its sensitivity level and reputation information from Symantec Insight in the cloud to determine that the file is not harmful.  
You use Internet Explorer to try to download a file. Download Insight uses its sensitivity level and reputation information from Symantec Insight in the cloud to determine that the file is not harmful.
- Download Insight determines that the file's reputation is acceptable, allows the file to download, and marks the file as a portal file.
- Later, Symantec gets more information about the file from its extensive global intelligence network. Symantec determines that the file might be harmful and updates the Insight reputation database. Symantec might provide a late-breaking signature for the file in its definitions in the cloud.
- If the user opens the file or runs a scan, Auto-Protect or the scan gets the latest information about the file from the cloud. Using the latest file reputation and the Download Insight sensitivity level, or using a late-breaking file signature, Auto-Protect or the scan now detects the file as potentially malicious.  
If you open the file or run a scan, Auto-Protect or the scan gets the latest information about the file from the cloud. Using the latest file reputation and the Download Insight sensitivity level, or using a late-breaking file signature, Auto-Protect or the scan now detects the file as potentially malicious.

### **Required and recommended settings**

**By default, Symantec Endpoint Protection uses the cloud. If you disable any of these options, you limit or disable cloud protection.**

- Auto-Protect  
Auto-Protect must be enabled. Auto-Protect is enabled by default.
- Download Insight  
Download Insight must be enabled so that it can examine file downloads, and so that file downloads are marked as portal files for future scans. If you disable Download Insight, all file downloads are treated as non-portal. Scans detect only the most malicious non-portal files.
- Insight lookups

---

Insight lookups must be enabled. The Insight lookups option controls reputation lookups as well as cloud definition lookups. This option is enabled by default.

**WARNING**

If you disable Insight lookups, cloud protection is completely disabled.

- Submissions

Symantec recommends that you share information with Symantec. Data you share with Symantec improves the performance of detection features. Information about the potential malware that might attack your computers helps improve the security landscape and address threats faster. Symantec makes every attempt to make the data pseudonymous to prevent the transmission of personally identifiable information.

[Understanding submissions to Symantec that improve protection on your computer](#)

## Managing scans on client computers

Some scans run by default, but you might want to change settings or set up your own scheduled scans. You can also customize scans and change how much protection they provide on your client computers.

Starting in 14, scans access the complete definitions set in the cloud.

[How Windows clients receive definitions from the cloud](#)

**Table 93: Modifying scans on client computers**

Task	Description
Review the types of scans and default settings	Check your scan settings. You can review the defaults and determine if you want to make changes. <a href="#">About the types of scans and real-time protection</a> <a href="#">About the default Virus and Spyware Protection policy scan settings</a>
Create scheduled scans and run on-demand scans	You use scheduled scans and on-demand scans to supplement the protection that Auto-Protect provides. Auto-Protect provides protection when you read and write files. Scheduled scans and on-demand scans can scan any files that exist on your client computers. They can also protect memory, load points, and other important locations on your client computers. You can save your scheduled scan settings as a template. The scan templates can save you time when you configure multiple policies. You can use any scan that you save as a template as the basis for a new scan in a different policy. <b>Note:</b> For managed clients, Symantec Endpoint Protection provides a default scheduled scan that scans all files, folders, and locations on the client computers. <a href="#">Setting up scheduled scans that run on Windows computers</a> <a href="#">Setting up scheduled scans that run on Mac computers</a> <a href="#">Setting up scheduled scans that run on Linux computers</a> <a href="#">Running on-demand scans on client computers</a>
Customize scan settings for your environment	You can customize Auto-Protect settings as well as options in administrator-defined scans. You might want to change scan settings to handle false positive detections, optimize computer or scan performance, or change scan actions or notifications. For scheduled scans, you can also set options for missed scans, randomized scans, and whether to scan network drives. <a href="#">Customizing the virus and spyware scans that run on Windows computers</a> <a href="#">Customizing the virus and spyware scans that run on Mac computers</a> <a href="#">Customizing the virus and spyware scans that run on Linux computers</a>

Task	Description
Adjust scans to improve client computer performance	<p>By default, Symantec Endpoint Protection provides a high level of security while it minimizes the effect on your client computers' performance. You can change some settings, however, to optimize the computer performance even more. Optimization is important in virtualized environments.</p> <p><b>Note:</b> When you adjust settings to optimize client computer performance, you might decrease some security on your client computers.</p> <p><a href="#">Adjusting scans to improve computer performance</a></p>
Adjust scans to increase protection on your client computers	<p>The default scan settings optimize your client computers' performance while still providing a high level of protection. You can increase the level of protection, however.</p> <p><a href="#">Adjusting scans to increase protection on your client computers</a></p>
Manage Download Insight detections	<p>Download Insight inspects files that users try to download through web browsers, text messaging clients, and other portals. Download Insight uses reputation information from Symantec Insight to make decisions about files.</p> <p><a href="#">Managing Download Insight detections</a></p>
Manage SONAR	<p>SONAR is part of Proactive Threat Protection on your client computers. However, SONAR settings are part of a Virus and Spyware Protection policy.</p> <p><a href="#">Managing SONAR</a></p>
Configure exceptions for scans	<p>You can create exceptions for the files and applications that you know are safe. Symantec Endpoint Protection also excludes some files and folders automatically.</p> <p><a href="#">Managing exceptions in Symantec Endpoint Protection</a></p> <p><a href="#">About the files and folders that Symantec Endpoint Protection excludes from virus and spyware scans</a></p>
Manage files in the Quarantine	<p>You can monitor and delete the files that are quarantined on your client computers. You can also specify settings for the Quarantine.</p> <p><a href="#">Managing the Quarantine for Windows clients</a></p>
Allow clients to submit information about detections to Symantec	<p>By default, clients send information about detections to Symantec. You can turn off submissions or choose which types of the information that clients submit. Symantec recommends that you always allow clients to send submissions. The information helps Symantec address threats.</p> <p><a href="#">Understanding server data collection and client submissions and their importance to the security of your network</a></p>
Manage the virus and spyware notifications that appear on client computers	<p>You can decide whether or not notifications appear on client computers for virus and spyware events.</p> <p><a href="#">Managing the virus and spyware notifications that appear on client computers</a></p>

## About the types of scans and real-time protection

Symantec Endpoint Protection includes different types of scans and real-time protection to detect different types of viruses, threats, and risks.

### NOTE

Starting in 14, scans access the complete definitions set in the cloud.

[How Windows clients receive definitions from the cloud](#)

By default, Symantec Endpoint Protection runs an active scan every day at 12:30 P.M. Symantec Endpoint Protection also runs an active scan when new definitions arrive on the client computer. On unmanaged computers, Symantec Endpoint Protection also includes a default startup scan that is disabled.

### NOTE

When a client computer is off or in hibernation or sleep mode, the computer might miss a scheduled scan. When the computer starts up or wakes, by default the scan is retried within a specified interval. If the interval already

expired, Symantec Endpoint Protection does not run the scan and waits until the next scheduled scan time. You can modify the settings for missed scheduled scans.

You should make sure that you run an active scan every day on the computers in your network. You might want to schedule a full scan once a week or once a month if you suspect that you have an inactive threat in your network. Full scans consume more computer resources and might affect computer performance.

#### [Managing scans on client computers](#)

**Table 94: Scan types**

Scan type	Description
Auto-Protect	<p>Auto-Protect continuously inspects files and email data as they are written to or read from a computer. Auto-Protect automatically neutralizes or eliminates detected viruses and security risks. Mac clients and Linux clients support Auto-Protect for the file system only.</p> <p>Starting in 14, on standard and embedded/VDI clients that are connected to the cloud, Auto-Protect automatically looks up the latest definitions in the cloud.</p> <p><a href="#">Customizing Auto-Protect for Linux clients</a></p>
Download Insight (Windows only)	<p>Download Insight boosts the security of Auto-Protect scans by inspecting files when users try to download them from browsers and other portals. It uses reputation information from Symantec Insight to allow or block download attempts.</p> <p>Download Insight functions as part of Auto-Protect and requires Auto-Protect to be enabled.</p> <p><a href="#">How Symantec Endpoint Protection uses Symantec Insight to make decisions about files</a></p>
Administrator-defined scans	<p>Administrator-defined scans detect viruses and security risks by examining all files and processes on the client computer. Administrator-defined scans can also inspect memory and load points.</p> <p><b>The following types of administrator-defined scans are available:</b></p> <ul style="list-style-type: none"><li>• <b>Scheduled scans</b> A scheduled scan runs on the client computers at designated times. Any concurrently scheduled scans run sequentially. If a computer is turned off or in hibernation or sleep mode during a scheduled scan, the scan does not run unless it is configured to retry missed scans. When the computer starts or wakes, Symantec Endpoint Protection retries the scan until the scan starts or the retry interval expires. You can schedule an active, full, or custom scan for Windows clients. You can schedule only a custom scan for Mac clients or Linux clients. You can save your scheduled scan settings as a template. You can use any scan that you save as a template as the basis for a different scan. The scan templates can save you time when you configure multiple policies. A scheduled scan template is included by default in the policy. The default scheduled scan scans all files and directories.</li><li>• <b>Startup scans and triggered scans</b> Startup scans run when the users log on to the computers. Triggered scans run when new virus definitions are downloaded to computers. <b>Note:</b> Startup scans and triggered scans are available only for Windows clients.</li><li>• <b>On-demand scans</b> On-demand scans are the scans that run immediately when you select the scan command in Symantec Endpoint Protection Manager. You can select the command from the <b>Clients</b> tab or from the logs.</li></ul> <p>If the Symantec Endpoint Protection client for Windows detects a large number of viruses, spyware, or high-risk threats, an aggressive scan mode engages. The scan restarts and uses Insight lookups.</p> <p>The scan may log detections at a higher sensitivity level than the policy defines for the duration of this scan.</p> <p><a href="#">Setting up scheduled scans that run on Windows computers</a></p> <p><a href="#">Setting up scheduled scans that run on Mac computers</a></p>

Scan type	Description
SONAR (Windows only)	<p>SONAR offers real-time protection against zero-day attacks. SONAR can stop attacks even before traditional signature-based definitions detect a threat. SONAR uses heuristics as well as file reputation data to make decisions about applications or files.</p> <p>Like proactive threat scans, SONAR detects keyloggers, spyware, and any other application that might be malicious or potentially malicious.</p> <p><a href="#">About SONAR</a></p>
Early launch anti-malware (ELAM) (Windows only)	<p>Works with the Windows early launch anti-malware driver. Supported only as of Windows 8 and Windows Server 2012.</p> <p>Early launch anti-malware provides protection for the computers in your network when they start up and before third-party drivers initialize.</p> <p><a href="#">Managing early launch anti-malware (ELAM) detections</a></p>

## About the types of Auto-Protect

Auto-Protect scans files as well as certain types of email and email attachments.

By default, all types of Auto-Protect are enabled. If you use a server-based email scanning solution such as Symantec Mail Security, you might not need to enable Auto-Protect for email.

Mac clients and Linux clients do not support email Auto-Protect scans.

**Table 95: Types of Auto-Protect**

Type of Auto-Protect	Description
Auto-Protect	<p>Continuously scans files as they are read from or written to the client computer. Auto-Protect is enabled by default for the file system. It loads at computer startup. It inspects all files for viruses and security risks, and blocks the security risks from being installed. It can optionally scan files by file extension, scan files on remote computers, and scan floppies for boot viruses. It can optionally back up files before it attempts to repair the files, and terminate processes and stop services.</p> <p>You can configure Auto-Protect to scan only selected file extensions. When Auto-Protect scans the selected extensions, it can also determine a file's type even if a virus changes the file's extension.</p> <p>For those clients that do not run email Auto-Protect, your client computers are still protected when Auto-Protect is enabled. Most email applications save attachments to a temporary folder when users launch email attachments. Auto-Protect scans the file as it is written to the temporary folder and detects any virus or security risk. Auto-Protect also detects the virus if the user tries to save an infected attachment to a local drive or network drive.</p>
Microsoft Outlook Auto-Protect (Windows only)	<p>Downloads incoming Microsoft Outlook email attachments and scans for viruses and security risks when the user reads the message and opens the attachment.</p> <p>The Outlook Auto-Protect plug-in supports Microsoft Outlook 98 through Outlook 2016 and Outlook 365 for the MAPI or Internet protocols. Outlook Auto-Protect supports 32-bit and 64-bit systems.</p> <p><b>Note:</b> If Microsoft Office 365 or Microsoft Office 2013 are installed with SEP 12.1.2 and earlier, and Microsoft Outlook 2016 installed with SEP 14, you may need to disable the Outlook Auto-Protect plug-in.</p> <p><b>Note:</b> <a href="#">Microsoft Outlook 365 stops working with Symantec Endpoint Protection client and Outlook add-in installed</a></p> <p><b>Note:</b> <a href="#">Outlook 2016 crashes when using the Endpoint Protection Add-in</a></p> <p>During installation, Symantec Endpoint Protection installs Microsoft Outlook Auto-Protect if you include it in the package and Microsoft Outlook is already installed on the computer.</p> <p>If a user downloads a large attachment over a slow connection, mail performance is affected. If you know the document is safe, you can create an exception.</p> <p><a href="#">Excluding a file or a folder from scans</a></p> <p><b>Note:</b> You should not install Microsoft Outlook Auto-Protect on a Microsoft Exchange Server. Instead you should install Symantec Mail Security for Microsoft Exchange.</p>
Internet Email Auto-Protect (Windows only) This feature is only available for client versions earlier than 14.2 RU1.	<p>Scans inbound Internet email body and email attachments for viruses and security risks; also performs outbound email heuristics scanning.</p> <p>By default, Internet Email Auto-Protect supports encrypted passwords and email over POP3 and SMTP connections. Internet Email Auto-Protect supports 32-bit or 64-bit systems. If you use POP3 or SMTP with Secure Sockets Layer (SSL), then the client detects secure connections but does not scan encrypted messages.</p> <p><b>Note:</b> For performance reasons, Internet Email Auto-Protect for POP3 is not supported on server operating systems.</p> <p>Email scanning does not support IMAP, AOL, or HTTP-based email such as Hotmail or Yahoo! Mail.</p>
Lotus Notes Auto-Protect (Windows only) This feature is only available for client versions earlier than 14.2 RU1.	<p>Scans incoming Lotus Notes email attachments for viruses and security risks.</p> <p>Lotus Notes Auto-Protect supports Lotus Notes 7.x or later.</p> <p>During installation, Symantec Endpoint Protection installs Lotus Notes Auto-Protect if you include it in the package and Lotus Notes is already installed on the computer.</p>

## About virus and security risks

Symantec Endpoint Protection scans for both viruses and for security risks. Viruses and security risks can arrive through email messages or instant messenger programs. Often a user unknowingly downloads a risk by accepting an End User License Agreement from a software program.

Many viruses and security risks are installed as drive-by downloads. These downloads usually occur when users visit malicious or infected Web sites, and the application's downloader installs through a legitimate vulnerability on the computer.

You can change the action that Symantec Endpoint Protection takes when it detects a virus or a security risk. For Windows clients, the security risk categories are dynamic and change over time as Symantec collects information about risks.

### [Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)

You can view information about specific virus and security risks on the Symantec Security Response Web site.

**Table 96: Viruses and security risks**

Risk	Description
Viruses	<p>Programs or code that attach a copy of themselves to another computer program or file when it runs. When the infected program runs, the attached virus program activates and attaches itself to other programs and files.</p> <p><b>The following types of threats are included in the virus category:</b></p> <ul style="list-style-type: none"><li>• Malicious Internet bots Programs that run automated tasks over the Internet. Bots can be used to automate attacks on computers or to collect information from Web sites.</li><li>• Worms Programs that replicate without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate in memory to reduce computer performance.</li><li>• Trojan horses Programs that hide themselves in something benign, such as a game or utility.</li><li>• Blended threats Threats that blend the characteristics of viruses, worms, Trojan horses, and code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. Blended threats use multiple methods and techniques to spread rapidly and cause widespread damage.</li><li>• Rootkits Programs that hide themselves from a computer's operating system.</li></ul>
Adware	Programs that deliver any advertising content.
Cookie	Messages that Web servers send to Web browsers for the purpose of identifying the computer or user.
Dialers	Programs that use a computer, without the user's permission or knowledge, to dial out through the Internet to a 900 number or FTP site. Typically, these numbers are dialed to accrue charges.
Hacking tools	Programs that hackers use to gain unauthorized access to a user's computer. For example, one hacking tool is a keystroke logger, which tracks and records individual keystrokes and sends this information back to the hacker. The hacker can then perform port scans or vulnerability scans. Hacking tools may also be used to create viruses.
Joke programs	Programs that alter or interrupt the operation of a computer in a way that is intended to be humorous or frightening. For example, a joke program might move the recycle bin away from the mouse when the user tries to delete an item.

Risk	Description
Misleading applications	Applications that intentionally misrepresent the security status of a computer. These applications typically masquerade as security notifications about any fake infections that must be removed.
Parental control programs	Programs that monitor or limit computer usage. The programs can run undetected and typically transmit monitoring information to another computer.
Remote access programs	Programs that allow access over the Internet from another computer so that they can gain information or attack or alter a user's computer.
Security assessment tool	Programs that are used to gather information for unauthorized access to a computer.
Spyware	Stand-alone programs that can secretly monitor system activity and detect passwords and other confidential information and relay it back to another computer.
Trackware	Stand-alone or appended applications that trace a user's path on the Internet and send information to the controller or hacker's system.

## About the files and folders that Symantec Endpoint Protection excludes from virus and spyware scans

When Symantec Endpoint Protection detects the presence of certain third-party applications and some Symantec products, it automatically creates exclusions for these files and folders. The client excludes these files and folders from all scans.

### NOTE

The client does not exclude the system temporary folders from scans because doing so can create a significant security vulnerability on a computer.

To improve scan performance or reduce false positive detections, you can exclude files by adding a file or a folder exception to an Exceptions policy. You can also specify the file extensions or the folders that you want to include in a particular scan.

### WARNING

The files or folders that you exclude from scans are not protected from viruses and security risks.

You can view the exclusions that the client automatically creates.

### Look in the following locations of the Windows registry:

- On 32-bit computers, see HKEY\_LOCAL\_MACHINE\Software\Symantec\Symantec Endpoint Protection\AV\Exclusions.
- On 64-bit computers, see HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Symantec\Symantec Endpoint Protection\AV\Exclusions.

### WARNING

Do not edit this registry directly.



**Table 97: File and folder exclusions**

Files	Description
Microsoft Exchange	<p><b>The client software automatically creates file and folder scan exclusions for the following Microsoft Exchange Server versions:</b></p> <ul style="list-style-type: none"> <li>• Exchange 5.5</li> <li>• Exchange 6.0</li> <li>• Exchange 2000</li> <li>• Exchange 2003</li> <li>• Exchange 2007</li> <li>• Exchange 2007 SP1</li> <li>• Exchange 2010</li> <li>• Exchange 2013</li> <li>• Exchange 2016</li> </ul> <p>For Exchange 2007, see your user documentation for information about compatibility with antivirus software. In a few circumstances, you might need to create scan exclusions for some Exchange 2007 folders manually. For example, in a clustered environment, you might need to create some exclusions. The client software checks for changes in the location of the appropriate Microsoft Exchange files and folders at regular intervals. If you install Microsoft Exchange on a computer where the client software is already installed, the exclusions are created when the client checks for changes. The client excludes both files and folders; if a single file is moved from an excluded folder, the file remains excluded. For more information, see the article, <a href="#">Preventing Symantec Endpoint Protection from scanning the Microsoft Exchange 2007 directory structure</a>.</p>
Microsoft Forefront	<p><b>The client automatically creates file and folder exclusions for the following Microsoft Forefront products:</b></p> <ul style="list-style-type: none"> <li>• Forefront Server Security for Exchange</li> <li>• Forefront Server Security for SharePoint</li> <li>• Forefront Threat Management Gateway</li> </ul> <p>Check the Microsoft Web site for a list of recommended exclusions. Also see the article, <a href="#">Configuring Symantec Endpoint Protection exclusions for Microsoft Forefront</a>.</p>
Active Directory domain controller	<p>The client automatically creates file and folder exclusions for the Active Directory domain controller database, logs, and working files. The client monitors the applications that are installed on the client computer. If the software detects Active Directory on the client computer, the software automatically creates the exclusions.</p>
Symantec products	<p>The client automatically creates appropriate file and folder scan exclusions for certain Symantec products when they are detected.</p> <p>The client creates exclusions for the following Symantec products:</p> <ul style="list-style-type: none"> <li>• Symantec Mail Security 4.0, 4.5, 4.6, 5.0, and 6.0 for Microsoft Exchange</li> <li>• Symantec AntiVirus/Filtering 3.0 for Microsoft Exchange</li> <li>• Norton AntiVirus 2.x for Microsoft Exchange</li> <li>• Symantec Endpoint Protection Manager default database (Microsoft SQL Server Express or embedded) and logs</li> </ul>
Veritas products	<p>The client automatically creates appropriate file and folder scan exclusions for certain Veritas products when they are detected:</p> <ul style="list-style-type: none"> <li>• Veritas Backup Exec</li> <li>• Veritas NetBackup</li> <li>• Veritas System Recovery</li> </ul> <p>Support for auto-exclusions of Veritas Netbackup ended with 8.x.</p>

Files	Description
Selected extensions and Microsoft folders	<p>For each type of administrator-defined scan or Auto-Protect, you can select files to include by extension. For administrator-defined scans, you can also select files to include by folder. For example, you can specify that a scheduled scan only scans certain extensions and that Auto-Protect scans all extensions. For executable files and Microsoft Office files, Auto-Protect can determine a file's type even if a virus changes the file's extension.</p> <p>By default, Symantec Endpoint Protection scans all extensions and folders. Any extensions or folders that you deselect are excluded from that particular scan.</p> <p>Symantec does not recommend that you exclude any extensions from scans. If you decide to exclude files by extension and any Microsoft folders, however, you should consider the amount of protection that your network requires. You should also consider the amount of time and resources that your client computers require to complete the scans.</p> <p><b>Note:</b> Any file extensions that you exclude from Auto-Protect scans of the file system also excludes the extensions from Download Insight. If you are running Download Insight, you should include extensions for common programs and documents in the list of extensions that you want to scan. You should also make sure that you scan .msi files.</p>
File and folder exceptions	<p>You use an Exceptions policy to create exceptions for the files or the folders that you want Symantec Endpoint Protection to exclude from all virus and spyware scans.</p> <p><b>Note:</b> By default, users on client computers can also create file and folder exceptions.</p> <p>For example, you might want to create file exclusions for an email application inbox. If the client detects a virus in the Inbox file during an on-demand or scheduled scan, the client quarantines the entire inbox. You can create an exception to exclude the inbox file instead. If the client detects a virus when a user opens an email message, however, the client still quarantines or deletes the message.</p>
Trusted files	<p>Virus and spyware scans use Insight, which lets scans skip trusted files. You can choose the level of trust for the files that you want to skip, or you can disable the option. If you disable the option, you might increase scan time.</p> <p>Auto-Protect can also skip the files that are accessed by trusted processes such as Windows Search.</p>

### Excluding a file or a folder from scans

## About the default Virus and Spyware Protection policy scan settings

Symantec Endpoint Protection Manager includes three default policies.

- Virus and Spyware Protection Balanced policy
- Virus and Spyware Protection High Security policy  
The High Security policy is the most stringent of all the preconfigured policies. You should be aware that it can affect the performance of other applications.
- Virus and Spyware Protection High Performance policy  
The High Performance policy provides better performance than the High Security policy, but it does not provide the same safeguards. The policy relies primarily on Auto-Protect to scan files with selected file extensions to detect threats.

The basic Virus and Spyware Protection policy provides a good balance between security and performance.

**Table 98: Virus and Spyware Protection Balanced policy scan settings**

Setting	Description
Auto-Protect for the file system	<p>Enabled</p> <p>Download Insight malicious file sensitivity is set to level 5.</p> <p>The Download Insight action for unproven files is <b>Ignore</b>.</p> <p><b>Auto-Protect includes the following settings:</b></p> <ul style="list-style-type: none"> <li>Scans all files for viruses and security risks.</li> <li>Blocks the security risks from being installed.</li> <li>Cleans the virus-infected files. Backs up the files before it repairs them. Quarantines the files that cannot be cleaned.</li> <li>Quarantines the files with security risks. Logs the files that cannot be quarantined.</li> <li>Checks all floppies for boot viruses. Logs the boot viruses.</li> <li>Notifies the computer users about viruses and security risks.</li> </ul>
Auto-Protect for email	<p>Enabled</p> <p><b>Other types of Auto-Protect include the following settings:</b></p> <ul style="list-style-type: none"> <li>Scans all files, including the files that are inside compressed files.</li> <li>Cleans the virus-infected files. Quarantines the files that cannot be cleaned.</li> <li>Quarantines the files with security risks. Logs the files that cannot be quarantined.</li> <li>Sends a message to the computer users about detected viruses and security risks.</li> </ul>
SONAR	<p>Enabled</p> <ul style="list-style-type: none"> <li>High risk heuristic detections are quarantined</li> <li>Logs any low risk heuristic detections</li> <li>Aggressive mode is disabled</li> <li><b>Show alert upon detection</b> is enabled</li> <li>System change detection actions are set to Ignore.</li> <li>Suspicious behavior detection blocks high risk threats and ignores low risk threats.</li> </ul>
Administrator-defined scans	<p><b>The scheduled scan includes the following default settings:</b></p> <ul style="list-style-type: none"> <li>Performs an active scan every day at 12:30 P.M. The scan is randomized.</li> <li>Scans all files and folders, including the files that are contained in compressed files.</li> <li>Scans memory, common infection locations, and known virus and security risk locations.</li> <li>Cleans the virus-infected files. Backs up the files before it repairs them. Quarantines the files that cannot be cleaned.</li> <li>Quarantines the files with security risks. Logs the files that cannot be quarantined.</li> <li>Retries missed scans within three days.</li> </ul> <p><b>The on-demand scan provides the following protection:</b></p> <ul style="list-style-type: none"> <li>Scans all files and folders, including the files that are contained in compressed files.</li> <li>Scans memory and common infection locations.</li> <li>Cleans the virus-infected files. Backs up the files before it repairs them. Quarantines the files that cannot be cleaned.</li> <li>Quarantines the files with security risks. Logs the files that cannot be quarantined.</li> </ul>

The default Virus and Spyware High Security policy provides high-level security, and includes many of the settings from the Virus and Spyware Protection policy. The policy provides increased scanning.

**Table 99: Virus and Spyware Protection High Security policy settings**

Setting	Description
Auto-Protect for the file system and email	Same as Virus and Spyware Protection Balanced policy Auto-Protect also inspects the files on the remote computers.
SONAR	<b>Same as Virus and Spyware Protection Balanced policy but with the following changes:</b> <ul style="list-style-type: none"><li>Blocks any system change events.</li></ul>
Global settings	Bloodhound is set to Aggressive. <b>Note:</b> The Aggressive option is likely to produce more false positives. This option is only recommended for advanced users.

The default Virus and Spyware Protection High Performance policy provides high-level performance. The policy includes many of the settings from the Virus and Spyware Protection policy. The policy provides reduced security.

**Table 100: Virus and Spyware Protection High Performance policy settings**

Setting	Description
Auto-Protect for the file system	<b>Same as Virus and Spyware Protection Balanced policy but with the following changes:</b> <ul style="list-style-type: none"><li>Download Insight malicious file sensitivity is set to level 1.</li></ul>
Microsoft Outlook Auto-Protect Internet Email Auto-Protect* Lotus Notes Auto-Protect* * Only available for client versions earlier than 14.2 RU1	Disabled
SONAR	<b>Same as Virus and Spyware Protection Balanced policy with the following changes:</b> <ul style="list-style-type: none"><li>Ignores any system change events.</li><li>Ignores any behavioral policy enforcement events.</li></ul>
Administrator-defined scans	Same as Virus and Spyware Protection Balanced policy.

## How Symantec Endpoint Protection handles detections of viruses and security risks

Symantec Endpoint Protection uses default actions to handle the detection of viruses and security risks. You can change some of the defaults.

**Table 101: How Symantec Endpoint Protection handles the detection of viruses and security risks**

Detection	Description
Viruses	By default, the Symantec Endpoint Protection client first tries to clean a file that a virus infects. <b>If the client software cannot clean the file, it does the following actions:</b> <ul style="list-style-type: none"><li>• Moves the file to the Quarantine on the infected computer</li><li>• Denies any access to the file</li><li>• Logs the event</li></ul>
Security risks	By default, the client moves any files that security risks infect to the Quarantine on the infected computer. The client also tries to remove or repair the risk's side effects. If a security risk cannot be quarantined and repaired, the second action is to log the risk. By default, the Quarantine contains a record of all actions that the client performed. You can return the client computer to the state that existed before the client tried the removal and repair.

Detections by SONAR are considered suspicious events. You configure actions for these detections as part of the SONAR configuration.

### Managing SONAR

For Windows clients and Linux clients, you can assign a first and a second action for Symantec Endpoint Protection to take when it finds risks. You can configure different actions for viruses and security risks. You can use different actions for scheduled, on-demand, or Auto-Protect scans.

As of 14.3 RU1, configuring the actions for detections is deprecated for the Linux client.

#### NOTE

Risky cookies are always deleted unless you specify that you want to log cookies instead. You can specify only one action for cookies, either **Delete** or **Leave alone (log only)**.

#### NOTE

On Windows clients, the list of the detection types for security risks is dynamic and changes as Symantec discovers new categories. New categories are downloaded to the console or the client computer when new definitions arrive.

For Mac clients, you can specify whether Symantec Endpoint Protection repairs the infected files that it finds. You can also specify whether Symantec Endpoint Protection moves the infected files that it cannot repair into the Quarantine. You can use different actions for scheduled, on-demand, or Auto-Protect scans.

### Managing the Quarantine for Windows clients

## How Symantec Endpoint Protection handles detections on Windows 8 computers

Symantec Endpoint Protection protects both the Windows 8 style user interface as well as the Windows 8 desktop. However, actions for the detections that are related to Windows 8 style apps and files function differently than actions for other detections.

The applications that are hosted on the Windows 8 style user interface are implemented in containers that are isolated from other processes in the operating system. Symantec Endpoint Protection does not clean or quarantine any detections that affect Windows 8 style apps or files. For any detections that involve these apps and files, Symantec Endpoint Protection only deletes or logs the detections.

For any detections that are not related to Windows 8 style apps and files, Symantec Endpoint Protection can quarantine and repair the detections and functions as it typically does on any other Windows operating system.

---

You should keep in mind the difference when setting up actions in Virus and Spyware Protection policy and when you run reports.

[About the pop-up notifications that appear on Windows 8 clients](#)

[How Symantec Endpoint Protection handles detections of viruses and security risks](#)

## Setting up scheduled scans that run on Windows computers

You configure scheduled scans as part of a Virus and Spyware Protection policy.

Consider the following important points when you set up a scheduled scan for the Windows computers in your security network:

Multiple simultaneous scans run serially	If you schedule multiple scans to occur on the same computer and the scans start at the same time, the scans run serially. After one scan finishes, another scan starts. For example, you might schedule three separate scans on your computer to occur at 1:00 P.M. Each scan scans a different drive. One scan scans drive C. Another scan scans drive D. Another scan scans drive E. In this example, a better solution is to create one scheduled scan that scans drives C, D, and E.
Missed scheduled scans might not run	If your computer misses a scheduled scan for some reason, by default Symantec Endpoint Protection tries to perform the scan until it starts or until a specific time interval expires. If Symantec Endpoint Protection cannot start the missed scan within the retry interval, it does not run the scan.
Scheduled scan time might drift	Symantec Endpoint Protection might not use the scheduled time if the last run of the scan occurred at a different time because of the scan duration or missed scheduled scan settings. For example, you might configure a weekly scan to run every Sunday at midnight and a retry interval of one day. If the computer misses the scan and starts up on Monday at 6 A.M., the scan runs at 6 A.M. The next scan is performed one week from Monday at 6 A.M. rather than the next Sunday at midnight. If you did not restart your computer until Tuesday at 6 A.M., which is two days late and exceeds the retry interval, Symantec Endpoint Protection does not retry the scan. It waits until the next Sunday at midnight to try to run the scan. In either case, if you randomize the scan start time you might change the last run time of the scan.

### NOTE

Windows settings include some options that are not available for clients that run on other operating systems.

You can click Help for more information about the options that are used in this procedure.

To set up scheduled scans that run on Windows computers

- 
1. In the console, open a Virus and Spyware Protection policy.
  2. Under **Windows Settings**, click **Administrator-defined Scans**.
  3. On the **Scans** tab, under **Scheduled Scans**, click **Add**.
  4. In the **Add Scheduled Scan** dialog box, click **Create a new scheduled scan**.
  5. Click **OK**.
  6. In the **Add Scheduled Scan** dialog box, on the **Scan Details** tab, type a name and description for this scheduled scan.
  7. Click **Active Scan**, **Full Scan**, or **Custom Scan**.
  8. If you selected **Custom**, under **Scanning**, you can specify the folders to scan.
  9. Under **File types**, click **Scan all files** or **Scan only selected extensions**.

#### NOTE

Scheduled scans always scan container files unless you disable the **Scan files inside compressed files** option under **Advanced Scanning Options** or you create specific exceptions for the container file extensions.

10. Under **Enhance the scan by checking**, check or uncheck **Memory**, **Common infection locations**, or **Well-known virus and security risk locations**.
11. On the **Schedule** tab, under **Scanning schedule**, set the frequency and the time at which the scan should run.  
The retry setting under **Missed Scheduled Scans** changes automatically according to whether you select **Daily**, **Weekly**, or **Monthly**.
12. Under **Missed Scheduled Scans**, you can disable the option to run a missed scan or you can change the retry interval.  
You can also specify a maximum scan duration before the scan pauses. You can also randomize scan start time.
13. If you want to save this scan as a template, check **Save a copy as a Scheduled Scan Template**.
14. Click **OK**.

[Managing scans on client computers](#)

[Customizing administrator-defined scans for clients that run on Windows computers](#)

[Excluding file extensions from virus and spyware scans on Windows clients and Linux clients](#)

## Setting up scheduled scans that run on Mac computers

You configure scheduled scans as part of a Virus and Spyware Protection policy.

[Managing scans on client computers](#)

[Customizing administrator-defined scans for clients that run on Mac computers](#)

#### NOTE

Mac settings do not include all the options that are available for clients that run on Windows.

To set up scheduled scans that run on Mac computers

- 
1. In the console, open a Virus and Spyware Protection policy.
  2. Under **Mac Settings**, click **Administrator-defined Scans**.
  3. On the **Scans** tab, under **Scheduled Scans**, click **Add**.
  4. In the **Add Scheduled Scan** dialog box, click **Create a new scheduled scan**, and then click **OK**.
  5. In the **Add Scheduled Scan** dialog box, on the **Scan Details** tab, type a name and a description for the scan.
  6. Under **Scan drives and folders**, specify the items to scan.
  7. On the **Schedule** tab, under **Scanning schedule**, set the frequency and the time at which the scan should run.

**NOTE**

Symantec does not recommend to run a scheduled scan more than once a day. Increasing the frequency of the scans or setting up multiple scheduled scans may cause performance issues.

8. If you want to save this scan as a template, check **Save a copy as a Scheduled Scan Template**.
9. Click **OK**.

## Setting up scheduled scans that run on Linux computers

You configure scheduled scans as part of a Virus and Spyware Protection policy.

### To set up scheduled scans that run on Linux computers

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Linux Settings**, click **Administrator-defined Scans**.
3. On the **Scans** tab, under **Scheduled Scans**, click **Add**.
4. In the **Add Scheduled Scan** dialog box, click **Add Scheduled Scan**.
5. In the **Add Scheduled Scan** dialog box, on the **Scan Details** tab, type a name and description for this scheduled scan.
6. Under **Folder types**, click **Scan all folders** or specify the folders to scan.
7. Under **File types**, click **Scan all files** or **Scan only selected extensions**.

As of 14.3 RU1, **Scan only selected extensions** option is not available.

**NOTE**

Scheduled scans always scan container files unless you disable the **Scan files inside compressed files** option or you create specific exceptions for the container file extensions.

8. Under **Additional options**, check or uncheck **Scan for security risks**.
9. On the **Schedule** tab, under **Scanning schedule**, set the frequency and the time at which the scan should run.  
The retry setting under **Missed Scheduled Scans** changes automatically according to whether you select **Daily**, **Weekly**, or **Monthly**.
10. Under **Missed Scheduled Scans**, you can disable the option to run a missed scan or you can change the retry interval.
11. If you want to save this scan as a template, check **Save a copy as a Scheduled Scan Template**.
12. Click **OK**.

[Managing scans on client computers](#)



---

## Running on-demand scans on client computers

You can run a manual, or on-demand, scan on client computers remotely from the management console. You might want to run an on-demand scan as part of your strategy to prevent and handle virus and spyware attacks on your client computers.

By default, an active scan runs automatically after you update definitions. You can configure an on-demand scan as a full scan or custom scan and then run the on-demand scan for more extensive scanning.

Settings for on-demand scans are similar to the settings for scheduled scans.

For Windows client computers, you can run an active, full, or custom on-demand scan. For Mac and Linux client computers, you can run only a custom on-demand scan.

The custom scan uses the settings that are configured for on-demand scans in the Virus and Spyware Protection policy.

### NOTE

If you issue a restart command on a client computer that runs an on-demand scan, the scan stops, and the client computer restarts. The scan does not restart.

You can run an on-demand scan from the Computer Status log or from the **Clients** tab in the console.

You can cancel all scans in progress and queued for selected clients from the Computer Status log. If you confirm the command, the table refreshes and you see that the cancel command is added to the command status table.

To run on-demand scans on client computers

1. In the console, click **Clients**.
2. Under **Clients**, right-click the group or clients that you want to scan.
3. Do one of the following actions:
  - Click **Run a command on the group > Scan**.
  - Click **Run command on computers > Scan**.

Click **Update Content and Scan** to update definitions and then run the scan in one step.

4. For Windows clients, select **Active Scan**, **Full Scan**, or **Custom Scan**, and then click **OK**.

[Managing scans on client computers](#)

[Preventing and handling virus and spyware attacks on client computers](#)

[Running commands on client computers from the console](#)

[What are the commands that you can run on client computers?](#)

## Adjusting scans to improve computer performance

By default, virus and spyware scans minimize the effect on your client computers' resources. You can change some scan settings to optimize the performance even more. Many of the tasks that are suggested here are useful in the environments that run Symantec Endpoint Protection in guest operating systems on virtual machines (VMs).

**Table 102: To adjust scans to improve computer performance on Windows computers**

Task	Description
Modify tuning and compressed files options for scheduled and on-demand scans	<p><b>You can adjust the following options for scheduled and on-demand scans:</b></p> <ul style="list-style-type: none"> <li>• <b>Change tuning options</b> You can change the scan tuning to <b>Best Application Performance</b>. When you configure a scan with this setting, scans can start but they only run when the client computer is idle. If you configure an Active Scan to run when new definitions arrive, the scan might not run for up to 15 minutes if the user is using the computer</li> <li>• <b>Change the number of levels to scan compressed files</b> The default level is 3. You might want to change the level to 1 or 2 to reduce scan time.</li> </ul> <p><a href="#">Customizing administrator-defined scans for clients that run on Windows computers</a></p>
Use resumable scans	<p>For computers in your network that have large volumes, scheduled scans can be configured as resumable scans.</p> <p>A scan duration option provides a specified period to run a scan. If the scan does not complete by the end of the specified duration, it resumes when the next scheduled scan period occurs. The scan resumes at the place where it stopped until the entire volume is scanned. Typically, you use the scan duration option on servers.</p> <p><b>Note:</b> Do not use a resumable scan if you suspect that the computer is infected. You should perform a full scan that runs until it scans the entire computer. You should also not use a resumable scan if a scan can complete before the specified interval.</p> <p><a href="#">Setting up scheduled scans that run on Windows computers</a></p>
Adjust Auto-Protect settings	<p>You can adjust some settings for Auto-Protect scans of the file system that might improve your client computers' performance.</p> <p><b>You can set the following options:</b></p> <ul style="list-style-type: none"> <li>• <b>File cache</b> Make sure that the file cache is enabled (the default is enabled). When the file cache is enabled, Auto-Protect remembers the clean files that it scanned and does not rescan them.</li> <li>• <b>Network settings</b> When Auto-Protect scans of remote computers are enabled, make sure that <b>Only when files are executed</b> is enabled.</li> </ul> <p><a href="#">Customizing Auto-Protect for Windows clients</a></p>
Allow all scans to skip trusted files	<p><b>Virus and spyware scans include an option called Insight that skips trusted files. By default, Insight is enabled. You can change the level of trust for the types of files that scans skip:</b></p> <ul style="list-style-type: none"> <li>• <b>Symantec and Community Trusted</b> This level skips files that are trusted by Symantec and the Symantec Community.</li> <li>• <b>Symantec Trusted</b> This level skips only files that are trusted by Symantec.</li> </ul> <p><a href="#">Modifying global scan settings for Windows clients</a></p>
Randomize scheduled scans	<p>In virtualized environments, where multiple virtual machines (VMs) are deployed, simultaneous scans create resource problems. For example, a single server might run 100 or more VMs. Simultaneous scans on those VMs drain resources on the server.</p> <p>You can randomize scans to limit the impact on your server.</p> <p><a href="#">Randomizing scans to improve computer performance in virtualized environments on Windows clients</a></p>
Use Shared Insight Cache in virtualized environments	<p>Shared Insight Cache eliminates the need to rescan the files that Symantec Endpoint Protection has determined are clean. You can use Shared Insight Cache for scheduled and manual scans on your client computers. Shared Insight Cache is a separate application that you install on a server or in a virtual environment.</p> <p><a href="#">Enabling the use of a network-based Shared Insight Cache</a></p>

Task	Description
Disable early launch anti-malware (ELAM) detection	Symantec Endpoint Protection ELAM works with Windows ELAM to provide protection against malicious startup drivers. <a href="#">Managing early launch anti-malware (ELAM) detections</a>

**Table 103: To adjust scans to improve computer performance on Mac computers**

Task	Description
Enable idle-time scan	Applies to scheduled scans on clients that run on Mac computers. This option configures scheduled scans to run only while the computer is idle. <a href="#">Customizing administrator-defined scans for clients that run on Mac computers</a>
Modify compressed files setting	Applies to Auto-Protect and on-demand scans. You can enable or disable the option, but you cannot specify the level of compressed files to scan. <a href="#">Customizing Auto-Protect for Mac clients</a>

**Table 104: To adjust scans to improve computer performance on Linux computers**

Task	Description
Scan by type of folder	The default is to scan all folder types. You can specify any of: <b>Root</b> , <b>Home</b> , <b>Bin</b> , <b>Usr</b> , <b>Etc</b> , and <b>Opt</b> . If you know that a folder is safe, you can uncheck it in the list.
Scan by file type	The default is to scan all files. If you know that a given extension is safe, you can remove it from the list.
Scan files inside compressed files	You can expand up to three levels to scan within compressed files. You might want to change the level to 1 or 2 to reduce scan time.
Scan for security risks	Lets you choose whether to scan for security risks. Security risks are updated through LiveUpdate. Scanning for security risks slows the scan down, but increases security. The default is to scan for security risks. To improve computer performance, uncheck this option.

#### [Managing scans on client computers](#)

## Adjusting scans to increase protection on your client computers

Symantec Endpoint Protection provides a high level of security by default. You can increase the protection even more. The settings are different for clients that run on Windows computers and clients that run on Mac and Linux computers.

### NOTE

If you increase the protection on your client computers, you might affect computer performance.

**Table 105: Adjusting scans to increase protection on Windows computers**

Task	Description
Lock scan settings	Some settings are locked by default; you can lock additional settings so that users cannot change the protection on their computers.
Modify settings for administrator-defined scans	<p><b>You should check or modify the following options:</b></p> <ul style="list-style-type: none"> <li>• <b>Scan performance</b> Set the scan tuning to <b>Best Scan Performance</b>. The setting, however, might affect your client computer performance. Scans run even if the computer is not idle.</li> <li>• <b>Scheduled scan duration</b> By default, scheduled scans run until the specified time interval expires and then resume when the client computer is idle. You can set the scan duration to <b>Scan until finished</b>.</li> <li>• <b>Warning!</b> Make sure that Insight Lookup is enabled. If you disable Insight lookups, cloud protection is completely disabled. Scheduled and on-demand scans always use the cloud to evaluate portal files. Auto-Protect also uses the cloud to evaluate portal files.</li> </ul> <p><a href="#">Customizing administrator-defined scans for clients that run on Windows computers</a>  <a href="#">How Windows clients receive definitions from the cloud</a></p>
Specify stronger scan detection actions	<p>Specify <b>Quarantine</b>, <b>Delete</b>, or <b>Terminate</b> actions for detections.</p> <p><b>Note:</b> Be careful when you use <b>Delete</b> or <b>Terminate</b> for security risk detections. The action might cause some legitimate applications to lose functionality.</p> <p><a href="#">Changing the action that Symantec Endpoint Protection takes when it makes a detection</a></p>
Increase the level of Bloodhound protection	<p>Bloodhound locates and isolates the logical regions of a file to detect virus-like behavior. You can change the detection level from <b>Automatic</b> to <b>Aggressive</b> to increase the protection on your computers. The <b>Aggressive</b> setting, however, is likely to produce more false positives.</p> <p><a href="#">Modifying global scan settings for Windows clients</a></p>
Adjust Auto-Protect settings	<p><b>You can change the following options:</b></p> <ul style="list-style-type: none"> <li>• <b>File cache</b> You can disable the file cache so that Auto-Protect rescans good files.</li> <li>• <b>Network settings</b> By default, files on network drives are scanned only when they are executed.</li> </ul> <p><a href="#">Customizing Auto-Protect for Windows clients</a></p>

**Table 106: Adjusting scans to increase protection on Mac and Linux computers**

Task	Description
Modify compressed file options for scans	<p>The default is to scan 3 levels deep in compressed files. To increase protection, leave it at 3 levels, or change it to 3 if it is at a lower level.</p> <p><a href="#">Customizing administrator-defined scans for clients that run on Mac computers</a>  <a href="#">Customizing administrator-defined scans for clients that run on Linux computers</a></p>
Lock Auto-Protect settings	<p>Some settings are locked by default; you can lock additional settings so that users cannot change the protection on their computers. On the Mac client and the Linux client, you can click <b>Enable Auto-Protect</b>, and then click the lock icon to lock the setting.</p> <p><a href="#">Customizing Auto-Protect for Mac clients</a>  <a href="#">Customizing Auto-Protect for Linux clients</a></p>
Specify stronger scan detection actions	<p>Specify <b>Quarantine</b> or <b>Delete</b> (Linux only) actions for detections.</p> <p>As of 14.3 RU1, configuring the actions for detections is deprecated for the Linux client.</p> <p><b>Note:</b> Be careful when you use <b>Delete</b> for security risk detections. The action might cause some legitimate applications to lose functionality.</p> <p><a href="#">Changing the action that Symantec Endpoint Protection takes when it makes a detection</a></p>

---

## Managing Download Insight detections

Auto-Protect includes a feature that is called Download Insight, which examines the files that users try to download through Web browsers, text messaging clients, and other portals.

Supported portals include Internet Explorer, Firefox, Microsoft Outlook, Outlook Express, Google Chrome, Windows Live Messenger, and Yahoo Messenger.

Download Insight determines that a downloaded file might be a risk based on evidence about the file's reputation. Download Insight is supported only for the clients that run on Windows computers.

### NOTE

If you install Auto-Protect for email on your client computers, Auto-Protect also scans the files that users receive as email attachments.

### [Managing scans on client computers](#)

**Table 107: Managing Download Insight detections**

Task	Description
Learn how Download Insight uses reputation data to make decisions about files	Download Insight uses reputation information exclusively when it makes decisions about downloaded files. It does not use signatures or heuristics to make decisions. If Download Insight allows a file, Auto-Protect or SONAR scans the file when the user opens or runs the file. <a href="#">How Symantec Endpoint Protection uses Symantec Insight to make decisions about files</a>
View the Download Risk Distribution report to view Download Insight detections	You can use the Download Risk Distribution report to view the files that Download Insight detected on your client computers. You can sort the report by URL, Web domain, or application. You can also see whether a user chose to allow a detected file.  <b>Note:</b> Risk details for a Download Insight detection show only the first portal application that attempted the download. For example, a user might use Internet Explorer to try to download a file that Download Insight detects. If the user then uses Firefox to try to download the file, the risk details show Internet Explorer as the portal.  The user-allowed files that appear in the report might indicate false positive detections. You can also specify that you receive email notifications about new user-allowed downloads. <a href="#">Setting up administrator notifications</a>  Users can allow files by responding to notifications that appear for detections. Administrators receive the report as part of a weekly report that Symantec Endpoint Protection Manager generates and emails. You must have specified an email address for the administrator during installation or configured as part of the administrator properties. You can also generate the report from the <b>Reports</b> tab in the console. <a href="#">Running and customizing quick reports</a>

Task	Description
Create exceptions for specific files or Web domains	<p>You can create an exception for an application that your users download. You can also create an exception for a specific Web domain that you believe is trustworthy.</p> <p><a href="#">Specifying how Symantec Endpoint Protection handles monitored applications on Windows clients</a>  <a href="#">Excluding a trusted web domain from scans on Windows clients</a></p> <p><b>Note:</b> If your client computers use a proxy with authentication, you must specify trusted Web domain exceptions for Symantec URLs. The exceptions let your client computers communicate with Symantec Insight and other important Symantec sites.</p> <p><b>For information about the recommended exceptions, see the following articles:</b></p> <ul style="list-style-type: none"> <li>• <a href="#">How to test connectivity to Insight and Symantec licensing servers</a></li> <li>• <a href="#">Required exclusions for proxy servers to allow Symantec Endpoint Protection to connect to Symantec reputation and licensing servers</a></li> </ul> <p>By default, Download Insight does not examine any files that users download from a trusted Internet or intranet site. You configure trusted sites and trusted local intranet sites on the <b>Windows Control Panel &gt; Internet Options &gt; Security</b> tab. When the <b>Automatically trust any file downloaded from an intranet site</b> option is enabled, Symantec Endpoint Protection allows any file that a user downloads from any sites in the lists.</p> <p>Symantec Endpoint Protection checks for updates to the Internet Options trusted sites list at user logon and every four hours.</p> <p><b>Note:</b> Download Insight recognizes only explicitly configured trusted sites. Wildcards are allowed, but non-routable IP address ranges are not supported. For example, Download Insight does not recognize 10.*.* as a trusted site. Download Insight also does not support the sites that are discovered by the <b>Internet Options &gt; Security &gt; Automatically detect intranet network</b> option.</p>
Make sure that Insight lookups are enabled	<p>Download Insight requires reputation data from Symantec Insight to make decisions about files. If you disable Insight lookups, Download Insight runs but detects only the files with the worst reputations. Insight lookups are enabled by default.</p> <p><a href="#">Customizing Download Insight settings</a></p>

Task	Description
Customize Download Insight settings	<p><b>You might want to customize Download Insight settings for the following reasons:</b></p> <ul style="list-style-type: none"> <li>• Increase or decrease the number of Download Insight detections. You can adjust the malicious file sensitivity slider to increase or decrease the number of detections. At lower sensitivity levels, Download Insight detects fewer files as malicious and more files as unproven. Fewer detections are false positive detections. At higher sensitivity levels, Download Insight detects more files as malicious and fewer files as unproven. More detections are false positive detections.</li> <li>• Change the action for malicious or unproven file detections. You can change how Download Insight handles malicious or unproven files. The specified action affects not only the detection but whether or not users can interact with the detection. For example, you might change the action for unproven files to <b>Ignore</b>. Then Download Insight always allows unproven files and does not alert the user.</li> <li>• Alert users about Download Insight detections. When notifications are enabled, the malicious file sensitivity setting affects the number of notifications that users receive. If you increase the sensitivity, you increase the number of user notifications because the total number of detections increases. You can turn off notifications so that users do not have a choice when Download Insight makes a detection. If you keep notifications enabled, you can set the action for unproven files to <b>Ignore</b> so that these detections are always allowed and users are not notified. Regardless of the notifications setting, when Download Insight detects an unproven file and the action is <b>Prompt</b>, the user can allow or block the file. If the user allows the file, the file runs automatically. When notifications are enabled and Download Insight quarantines a file, the user can undo the quarantine action and allow the file.</li> </ul> <p><b>Note:</b> If users allow a quarantined file, the file does not automatically run. The user can run the file from the Temporary Internet Files folder. Typically, the folder location is one of the following:</p> <ul style="list-style-type: none"> <li>— Windows 8 and later: Drive:\Users\username\AppData\Local\Microsoft\Windows\INetCache</li> <li>— Windows Vista / 7: Drive:\Users\username\AppData\Local\Microsoft\Windows\Temporary Internet Files</li> </ul> <p><a href="#">Customizing Download Insight settings</a></p>
Allow clients to submit information about reputation detections to Symantec	<p>By default, clients send information about reputation detections to Symantec. Symantec recommends that you enable submissions for reputation detections. The information helps Symantec address threats.</p> <p><a href="#">Managing the pseudonymous or non-pseudonymous data that clients send to Symantec</a></p>

## How Symantec Endpoint Protection uses Symantec Insight to make decisions about files

Symantec collects information about files from its global community of millions of users and its Global Intelligence Network. The collected information is available to Symantec products in the cloud through Symantec Insight. Symantec Insight provides a file reputation database and the latest virus and spyware definitions.

Symantec products leverage Insight to protect client computers from new, targeted, and mutating threats. The data is sometimes referred to as being in the cloud since it does not reside on the client computer. Symantec Endpoint Protection must request or query Insight for information. The queries are called reputation lookups, cloud lookups, or Insight lookups.

### Insight reputation ratings

Symantec Insight determines each file's level of risk or security rating. The rating is also known as the file's reputation.

Insight determines a file's security rating by examining the following characteristics of a file and its context:

- 
- The source of the file
  - How new the file is
  - How common the file is in the community
  - Other security metrics, such as how the file might be associated with malware

### Insight lookups

Scanning features in Symantec Endpoint Protection leverage Insight to make decisions about files and applications. Virus and Spyware Protection includes a feature that is called Download Insight. Download Insight requires reputation information to make detections. SONAR also uses reputation information to make detections.

You can change the Insight lookups setting on the **Clients** tab. Go to **Policies > Settings > External Communications > Client Submissions**.

You can change the Insight lookups setting. Go to **Change Settings > Client Management > Submissions**.

Starting in 14, on standard and embedded/VDI clients, the Insight lookups option also allows Auto-Protect and scheduled and manual scans to look up file reputation information as well as definitions in the cloud. Symantec recommends that you keep the option enabled.

### WARNING

Download Insight, SONAR, and virus and spyware scans use Insight lookups for threat detection. Symantec recommends that you always allow Insight lookups. Disabling lookups disables Download Insight and impairs the functionality of SONAR heuristics and virus and spyware scans.

### File reputation submissions

By default, a client computer sends information about reputation detections to Symantec Security Response for analysis. The information helps to refine Insight's reputation database and the latest definitions in the cloud. The more clients that submit information the more useful the reputation database becomes.

Symantec recommends that you keep client submissions for reputation detections enabled.

## How does Symantec Endpoint Protection use advanced machine learning?

- [How does advanced machine learning work?](#)
- [How does AML work with the cloud?](#)
- [How do I configure AML?](#)
- [Troubleshooting advanced machine learning](#)

### How does advanced machine learning work?

The advanced machine learning (AML) engine determines if a file is good or bad through a learning process. Symantec Security Response trains the engine to recognize malicious attributes and defines the rules that the AML engine uses to make detections. Symantec trains and tests the AML engine in a lab environment using the following process:

- LiveUpdate downloads the AML model to the client and runs for several days.
- The AML engine learns which applications the client runs and get exploited using the client's telemetry data. Each client computer is part of the global intelligence network that returns information about the model to Symantec.
- Symantec adjusts the AML model based on what Symantec learns from the clients' telemetry data.
- Symantec modifies the AML model to block the applications that exploits typically attack.

AML is part of the static data scanner (SDS) engine. The SDS engine includes the emulator, the Intelligent Threat Cloud Service (ITCS), and the CoreDef-3 definitions engine.

Symantec Endpoint Protection uses advanced machine learning in Download Insight, SONAR, and virus and spyware scans, all which use Insight lookups for threat detection.



## How does AML work with the cloud?

Symantec leverages the Intelligent Threat Cloud Service (ITCS) to confirm the detection that AML makes on the client computer is correct. Sometimes AML may reverse the conviction after it checks with the ITCS. While the AML engine does not need Symantec Insight, this feedback enables Symantec to train the AML algorithms to reduce false positives and increase true positives. When the computer is online, Symantec Endpoint Protection can stop an average of 99% of threats.

[How Windows clients receive definitions from the cloud](#)

[How does the emulator in Symantec Endpoint Protection detect and clean malware?](#)

## How do I configure AML?

You cannot configure advanced machine learning. LiveUpdate downloads the AML definitions by default. However, you do need to make sure that the following technologies are enabled.

**Table 108: Steps to ensure that AML protects the client computers**

Task	Description
Step 1: Make sure that cloud lookup availability is enabled	<p>The queries that AML makes to Symantec Insight are called reputation lookups, cloud lookups, or Insight lookups. If Insight lookups are enabled, the AML detections for SONAR and virus and spyware scans have fewer false positives.</p> <p>To verify that Insight lookups are enabled, see:</p> <p><a href="#">How Symantec Endpoint Protection uses Symantec Insight to make decisions about files</a></p> <p>In addition, make sure that client submissions are enabled. This information helps Symantec measure and improve the effectiveness of detection technologies.</p> <p><a href="#">Understanding server data collection and client submissions and their importance to the security of your network</a></p>
Step 2: Make sure that Bloodhound Detections are enabled	<p>Set the Bloodhound Detection level to either automatic or aggressive.</p> <p><a href="#">Modifying global scan settings for Windows clients</a></p> <p>When the AML engine encounters certain high-risk files, the client automatically engages a more aggressive scan.</p> <p>When aggressive scan mode engages:</p> <ul style="list-style-type: none"><li>• The scan restarts.</li><li>• The following notification appears on the client:</li></ul> <p><code>Running an aggressive scan that uses Insight lookups to clean your computer.</code></p> <p>In the aggressive mode, you may need to further manage the false positives.</p>
Step 3: Make sure that LiveUpdate downloads high intensity definitions (14.0.1) (optional)	<p>LiveUpdate always downloads AML content.</p> <p>As of 14.0.1, LiveUpdate downloads a more aggressive set of definitions that work with the low bandwidth policy you get from the cloud. You can disable AML content from being downloaded through LiveUpdate.</p> <p>From LiveUpdate to Symantec Endpoint Protection Manager:</p> <p><a href="#">Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager</a></p> <p>From Symantec Endpoint Protection Manager to the Windows clients:</p> <p><a href="#">Reverting to an older version of the Symantec Endpoint Protection security updates</a></p> <p><a href="#">About the types of content that LiveUpdate downloads</a></p>
Step 4: Handle false positives	<p>Manage the false positives using the Exceptions policy.</p> <p><a href="#">Creating exceptions for Virus and Spyware scans</a></p> <p><a href="#">Handling and preventing SONAR false positive detections</a></p> <p><a href="#">Best Practice when Symantec Endpoint Protection is Detecting a File that is Believed to be Safe</a></p>

## Troubleshooting advanced machine learning

The logs and reports for advanced machine learning detections are the same as for the other SDS engines. To see a report with recent threats, run a Risk report for **New Risks Detected in the Network**.

---

As of 14.0.1, you can run a scheduled report for AML detections. On the **Reports** page, click **Scheduled Reports > Add > Computer Status > Advanced Machine Learning (Static) Content Distribution**. The Symantec Endpoint Protection Manager domain must be enrolled in the cloud console for the report to appear.

[How to run scheduled reports](#)

[Viewing logs](#)

## How does the emulator in Symantec Endpoint Protection detect and clean malware?

Symantec Endpoint Protection 14 introduced a powerful new emulator to protect against malware from custom packer attacks. For Auto-Protect and virus scans, this emulator improves scan performance and effectiveness by at least 10 percent from previous releases. This anti-evasion technique addresses packed malware obfuscation techniques and detects the malware that is hidden inside custom packers.

### What are custom packers?

Many malware programs make use of “packers,” or the software programs that are used to compress and encrypt files for transport. These files are then executed in memory upon arrival on the user's computer.

While packers themselves are not malware, attackers use them to hide malware and obfuscate the code's real intention. Once the malware is unpacked, it executes and launches its malicious payload, often bypassing firewalls, gateways, and malware protection. Attackers have shifted from using commercial packers (such as UPX, PECompact, ASProtect, and Themida) to creating custom packers. The custom packers use proprietary algorithms to bypass standard detection techniques.

Many of the emerging custom packers are polymorphic. They use an anti-detection strategy whereby the code itself changes frequently, but the purpose and functionality of the malware remains the same. Custom packers also use clever ways of injecting the code into a target process and change its execution flow, frequently throwing off unpacker routines. Some of them are computationally intensive, calling special APIs that make the unpacking difficult.

Custom packers have grown increasingly sophisticated to hide the attack until it's too late.

### How does the Symantec Endpoint Protection emulator protect against custom packers?

The high-speed emulator in Symantec Endpoint Protection fools malware into thinking it runs on the regular computer. Instead, the emulator unpacks and detonates the custom-packed file in a lightweight virtual sandbox on the client computer. The malware then opens up its payload in full, causing threats to reveal themselves in a contained environment. A static data scanner, which includes the antivirus engine and heuristics engine, acts on the payload. The sandbox is ephemeral and goes away after the threat is dealt with.

The emulator requires sophisticated technology that mimics operating systems, APIs, and processor instructions. It simultaneously manages the virtual memory and runs various heuristics and detection technologies to examine the payload. It takes an average of 3.5 milliseconds for clean files and 300 milliseconds for malware, at about the same time it takes client users to click a file on their desktop. The emulator can detect threats quickly with minimal performance and productivity impact, so client users are not interrupted. In addition, the emulator uses a minimal amount of disk space, a maximum of 16 MB memory in the virtual environment.

The emulator works with other protection techniques, which include advanced machine learning, memory exploit mitigation, behavior monitoring, and reputation analysis. Sometimes multiple engines come into play, collaborating in a response to prevent, detect, and remediate attacks.

The emulator does not use the Internet. However, the engines within the static data scanner may require the Internet based on the malware that the emulator extracted out of the custom packer.

[How does Symantec Endpoint Protection use advanced machine learning?](#)

[How do I configure the emulator?](#)

---

The emulator is built into the Symantec Endpoint Protection software so you don't need to configure it. Symantec regularly adds or changes the emulator content for new threats and releases quarterly content updates to the emulator engine. By default, LiveUpdate automatically downloads this content with the virus and spyware definitions.

#### [Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager](#)

Symantec Endpoint Protection Manager does not include separate logs for the detections that the emulator makes. Instead, you can find any detections in the Risk log and Scan log.

#### [Viewing logs](#)

## Managing the quarantine for Windows clients

You manage quarantine settings as an important part of your virus outbreak strategy.

When virus and spyware scans or SONAR detects a threat, Symantec Endpoint Protection places the suspicious files in the infected computer's local quarantine. The client either repairs the file, repairs and restores it, or deletes it.

When the client detects a risk and quarantines the file, the client notifies the management server. You can enable the management server to automatically request and retrieve the quarantined file. The management server uploads and stores risk samples in the database, displays their event details, and lets you download them for further analysis. You may want to submit the file to your internal malware or security team for reverse engineering, or to another sandbox for analysis. If you think the conviction is a false positive, contact Symantec Support to log a case.

### NOTE

Version 14 and later does not include the Central Quarantine Server.

As of 14.3 RU2, you can no longer use the Central Quarantine Server. Instead, the client submits quarantined files to the Symantec Endpoint Protection Manager.

### Upload quarantined files to the management server

The management server does not retrieve quarantined files from the client by default. You must enable this setting.

1. In the console, click **Admin > Domains > Edit Domain Properties**.
2. On the **General** tab, click **Upload quarantined files from the clients**, and then click **OK**.

To download files that the client quarantined and uploaded to the management server:

1. In the console, click **Monitors > Logs >** and select the **Risk** log type.
2. Open the log, select the quarantined file, and in the **Action** drop-down list, click **Download file that the client quarantined**.

### Configure the quarantine settings

You can modify the following options for how the quarantine treats files on the client:

- What happens when new definitions arrive on clients:  
By default, the client rescans items in the quarantine and automatically repairs and restores items silently when new definitions arrive. If you created an exception for a file or application in the quarantine, Symantec Endpoint Protection restores the file after new definitions arrive.
- Where quarantined items are stored:  
By default, the quarantine stores backup, repaired, and quarantined files in a default folder. The quarantine clean-up feature automatically deletes the files in the quarantine when the files exceed a specified age or when the directory where they are stored reaches a certain size. It automatically deletes files after 30 days.  
If you do not want to use the default quarantine directory (%ProgramData%\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Quarantine ) to store quarantined files on client computers, you can

---

specify a different local directory. You can use path expansion by using the percent sign when you type the path. For example, you can type %COMMON\_APPDATA%. Relative paths are not allowed.

1. In the Virus and Spyware Protection policy, click **Windows Settings > Quarantine**.
2. On the **General** tab, configure the options under **When New Virus Definitions Arrive** and **Local Quarantine Options**.

Specify how to handle quarantined items and which local folder to store quarantined files.

[Quarantine: General](#)

3. Click **OK**.

### Delete files in the quarantine

The quarantine automatically deletes repaired files, backup files, and quarantined files after a specified number of days. You can configure the quarantine to delete files when the folder where the files are stored reaches a specified size or after a certain number of days.

You should periodically check the client computer's quarantine to prevent accumulating a large numbers of files. Check the quarantined files when a new virus outbreak appears on the network.

Leave files with unknown infections in the quarantine. When the client receives new definitions, it rescans the items in the quarantine and might delete or repair the file.

You can delete a quarantined file if a backup exists or if you have a copy of the file from a trustworthy source. You can delete a quarantined file directly on the infected computer, or by using the Risk log in the Symantec Endpoint Protection console.

#### NOTE

If Symantec Endpoint Protection detects risks in a compressed file, the compressed file is quarantined as a whole. However, the Risk log contains a separate entry for each file in the compressed file. To successfully delete all risks in a compressed file, you must select all the files in the compressed file.

To configure the client to delete files automatically:

1. In the Virus and Spyware Protection policy, click **Windows Settings > Quarantine**.
2. On the **Cleanup** tab, check or uncheck the options to enable or disable them, and configure the time interval and size maximums.

[Quarantine: Cleanup](#)

3. Click **OK**.

To delete files from the Risk log:

1. In the console, click **Monitors**.
2. On the **Logs** tab, from the **Log type** list box, select the **Risk** log, and then click **View Log**.
3. Do one of the following actions:
  - Select an entry in the log that has a file that has been quarantined.
  - Select all entries for files in the compressed file.

You must have all entries in the compressed file in the log view. You can use the **Limit** option under **Additional Settings** to increase the number of entries in the view.
4. From the **Action** list box, select: **Delete from Quarantine**.
5. Click **Start**.
6. In the dialog box that appears, click **Delete**, and then **OK**.

## Managing the virus and spyware notifications that appear on client computers

You can decide whether or not notifications appear on client computers for virus and spyware events. You can customize messages about detections.

### [Managing scans on client computers](#)

**Table 109: Tasks for managing virus and spyware notifications that appear on client computers**

Task	Description
Customize a scan detection message	<p><b>For Windows and Linux client computers, you can configure a detection message for the following types of scans:</b></p> <ul style="list-style-type: none"><li>• All types of Auto-Protect</li><li>• Scheduled scans and on-demand scans</li></ul> <p>For scheduled scans, you can configure a separate message for each scan.</p> <p><b>Note:</b> If a process continually downloads the same security risk to a client computer, Auto-Protect automatically stops sending notifications after three detections. Auto-Protect also stops logging the event. In some situations, however, Auto-Protect does not stop sending notifications and logging events. Auto-Protect continues to send notifications and log events when the action for the detection is <b>Leave alone (log only)</b>.</p> <p>For Mac client computers, you can configure a detection message that applies to all scheduled scans, to on-demand scans, and to Auto-Protect detections. These notification messages appear in the macOS Notification Center. You cannot customize the messages for Mac.</p> <p><a href="#">Customizing administrator-defined scans for clients that run on Windows computers</a></p> <p><a href="#">Customizing administrator-defined scans for clients that run on Mac computers</a></p> <p><a href="#">Customizing administrator-defined scans for clients that run on Linux computers</a></p>
Change settings for user notifications about Download Insight detections	<p>Applies to Windows client computers only.</p> <p>You can change the notifications that users receive about Download Insight detections.</p> <p><a href="#">Managing Download Insight detections</a></p>
Change settings for user notifications about SONAR detections	<p>Applies to Windows client computers only.</p> <p>You can change the notifications that users receive about SONAR detections.</p> <p><a href="#">Managing SONAR</a></p>
Choose whether or not to display the Auto-Protect results dialog	<p>Applies to Windows client computers only.</p> <p>Applies to Auto-Protect for the file system only.</p> <p><a href="#">Customizing administrator-defined scans for clients that run on Windows computers</a></p>
Set up Auto-Protect email notifications	<p>Applies to Windows client computers only.</p> <p>When Auto-Protect email scans find a risk, Auto-Protect can send email notifications to alert the email sender and any other email address that you specify. You can also insert a warning into the email message.</p> <p>For Internet Email Auto-Protect, you can also specify that a notification appears about scan progress when Auto-Protect scans an email. Internet Email Auto-Protect is available only to client versions earlier than 14.2 RU1.</p> <p><a href="#">Customizing Auto-Protect for email scans on Windows computers</a></p>
Allow users to see scan progress and start or stop scans	<p>Applies to Windows client computers only.</p> <p>You can configure whether or not the scan progress dialog box appears. You can configure whether or not users are allowed to pause or delay scans.</p> <p>When you let users view scan progress, a link to the scan progress dialog appears in the main pages of the client user interface. A link to reschedule the next scheduled scan also appears.</p> <p><a href="#">Allowing users to view scan progress and interact with scans on Windows computers</a></p>

Task	Description
Configure warnings, errors, and prompts	Applies to Windows client computers only. You can enable or disable several types of alerts that appear on client computers about Virus and Spyware Protection events. <a href="#">Modifying log handling and notification settings on Windows computers</a>
Enable or disable popup notifications on the Windows 8 style user interface	Applies to clients that run on Windows 8. You can enable or disable the popup notifications that appear in the Windows 8 style user interface for detections and other critical events. <a href="#">Enabling or disabling Symantec Endpoint Protection pop-up notifications that appear on Windows 8 clients</a>

## About the pop-up notifications that appear on Windows 8 clients

On Windows 8 computers, pop-up notifications for malware detections and other critical Symantec Endpoint Protection events appear on the Windows 8 style user interface and the Windows 8 desktop. The notifications alert the user to an event that occurred in either the Windows 8 style user interface or the Windows 8 desktop, regardless of which interface the user is currently viewing.

You can enable or disable the pop-up notifications on your client computers.

### NOTE

The Windows 8 configuration also includes settings to show or hide notifications. Symantec Endpoint Protection pop-up notifications only appear if Windows 8 is configured to show them. In the Windows 8 style user interface, the **Settings** pane or the **Change PC Settings** option let you show or hide app notifications. See the Windows 8 user documentation for more information.

If the user clicks a notification on the Windows 8 style user interface, the Windows 8 desktop appears. If the user clicks the notification on the Windows 8 desktop, the notification disappears. For detections of malware or security risks, the user can view information about the detections in the **Detection Results** dialog on the Windows 8 desktop.

When Symantec Endpoint Protection notifies Windows 8 that it detected malware or a security risk that affects a Windows 8 style app, an alert icon appears on the app tile. When the user clicks the tile, the Windows App Store appears so that the user can re-download the app.

[Enabling or disabling Symantec Endpoint Protection pop-up notifications that appear on Windows 8 clients](#)

[How Symantec Endpoint Protection handles detections on Windows 8 computers](#)

## Enabling or disabling Symantec Endpoint Protection pop-up notifications that appear on Windows 8 clients

By default, pop-up notifications appear on the Windows 8 style user interface and the Windows 8 desktop for malware detections and other critical Symantec Endpoint Protection events.

The user can view the Windows desktop to see details about the event that produced the notification. The user might need to take an action such as re-download an app. In some cases, however, you might want to hide these pop-up notifications from users. You can enable or disable this type of notification in the Symantec Endpoint Protection configuration.

### NOTE

The Windows 8 configuration also includes settings to show or hide notifications. Symantec Endpoint Protection notifications only appear if Windows 8 is configured to show them. On the Windows 8 style user interface, the **Settings** pane or the **Change PC Settings** option let you show or hide app notifications. See the Windows 8 user documentation for more information.

---

To enable or disable Symantec Endpoint Protection notifications that appear on Windows 8 clients

1. In the console, on the **Clients** tab, on the **Policies** tab, under **Location-specific settings**, next to **Client User Interface Control Settings**, click **Server Control**.
2. Next to **Server Control**, click **Customize**.
3. In the **Client User Interface Settings** dialog, under **General**, check or uncheck **Enable Windows toast notifications**.
4. Click **OK**.

[About the pop-up notifications that appear on Windows 8 clients](#)

## Managing early launch anti-malware (ELAM) detections

Early launch anti-malware (ELAM) provides protection for the computers in your network when they start up and before third-party drivers initialize. Malicious software can load as a driver or rootkits might attack before the operating system completely loads and Symantec Endpoint Protection starts. Rootkits can sometimes hide themselves from virus and spyware scans. Early launch anti-malware detects these rootkits and bad drivers at startup.

### NOTE

ELAM is only supported on Microsoft Windows 8 or later, and Windows Server 2012 or later.

Symantec Endpoint Protection provides an ELAM driver that works with the Windows ELAM driver to provide the protection. The Windows ELAM driver must be enabled for the Symantec ELAM driver to have any affect.

You use the Windows Group Policy editor to view and modify the Windows ELAM settings. See your Windows documentation for more information.

**Table 110: Managing ELAM detections**

Task	Description
View the status of ELAM on your client computers	You can see whether Symantec Endpoint Protection ELAM is enabled in the Computer Status log. <a href="#">Viewing logs</a>
View ELAM detections	You can view early launch anti-malware detections in the Risk log. When Symantec Endpoint Protection ELAM is configured to report detections of bad or bad critical drivers as unknown to Windows, Symantec Endpoint Protection logs the detections as <b>Log only</b> . By default, Windows ELAM allows unknown drivers to load.
Enable or disable ELAM	You might want to disable Symantec Endpoint Protection ELAM to help improve computer performance. <a href="#">Adjusting the Symantec Endpoint Protection early launch anti-malware (ELAM) options</a> <a href="#">Adjusting scans to improve computer performance</a>
Adjust ELAM detection settings if you get false positives	The Symantec Endpoint Protection ELAM settings provide an option to treat bad drivers and bad critical drivers as unknown. Bad critical drivers are the drivers that are identified as malware but are required for computer startup. You might want to select the override option if you get false positive detections that block an important driver. If you block an important driver, you might prevent client computers from starting up.  <b>Note:</b> ELAM does not support a specific exception for an individual driver. The override option applies globally to ELAM detections.  <a href="#">Adjusting the Symantec Endpoint Protection early launch anti-malware (ELAM) options</a>



Task	Description
Run Power Eraser on ELAM detections that Symantec Endpoint Protection cannot remediate	In some cases, an ELAM detection requires Power Eraser. In those cases, a message appears in the log suggesting that you run Power Eraser. You can run Power Eraser from the console. Power Eraser is also part of the Symantec Help tool. You should run Power Eraser in rootkit mode. <a href="#">Starting Power Eraser analysis from Symantec Endpoint Protection Manager</a> <a href="#">Troubleshooting computer issues with the Symantec Diagnostic Tool (SymDiag)</a>

## Adjusting the Symantec Endpoint Protection early launch anti-malware (ELAM) options

Symantec Endpoint Protection provides an ELAM driver that works with the Microsoft ELAM driver to provide protection for the computers in your network when they start up. The settings are supported as of Microsoft Windows 8 and Windows Server 2012.

The Symantec Endpoint Protection ELAM driver is a special type of driver that initializes first and inspects other startup drivers for malicious code. When the driver detects a startup driver, it determines whether the driver is good, bad, or unknown. The Symantec Endpoint Protection driver then passes the information to Windows to decide to allow or block the detected driver.

You cannot create exceptions for individual ELAM detections; however, you can create a global exception to log all bad drivers as unknown. By default, unknown drivers are allowed to load.

For some ELAM detections that require remediation, you might be required to run Power Eraser. Power Eraser is part of the Symantec Help tool.

### NOTE

Auto-Protect scans any driver that loads.

To adjust the Symantec Endpoint Protection ELAM options

1. In the Symantec Endpoint Protection Manager console, on the **Policies** tab, open a Virus and Spyware Protection policy.
2. Under **Protection Technologies**, select **Early Launch Anti-Malware Driver**.
3. Check or uncheck **Enable Symantec early launch anti-malware**.

The Windows ELAM driver must be enabled for this option to be enabled. You use the Windows Group Policy editor or the registry editor to view and modify the Windows ELAM settings. See your Windows documentation for more information.

4. If you want to log the detections only, under **Detection Settings**, select **Log the detection as unknown so that Windows allows the driver to load**.
5. Click **OK**.

[Managing early launch anti-malware \(ELAM\) detections](#)

[Troubleshooting computer issues with the Symantec Diagnostic Tool \(SymDiag\)](#)

## Configuring a site to use a private Insight server for reputation queries

Private Insight server settings let you direct client reputation queries to an intranet server, if you have purchased and installed Symantec Insight for Private Clouds. Symantec Insight for Private Clouds is typically installed in networks that lack Internet connectivity. The private Insight server stores a copy of Symantec Insight's reputation database. Symantec Endpoint Protection reputation queries are handled by the private Insight server rather than Symantec's Insight server.



---

The private server downloads the Symantec Insight data over an encrypted, secure connection. You can manually update the Insight data or use third-party tools to check for updates and download the data automatically. Your update method depends on your network and the type of server on which you run Symantec Insight for Private Clouds.

When you use a private Insight server, Symantec does not receive any queries or submissions for file reputation.

To configure a site to use a private Insight server for reputation queries

1. In the console, on the **Admin** page, select **Servers**.
2. Select the site, and then under **Tasks**, select **Edit Site Properties**.
3. On the **Private Insight Server** tab, make sure that you check **Enable private Insight server**.

You must also enter the **Name**, **Server URL**, and **Port** number.

#### **NOTE**

If you change an existing Server URL to an invalid URL, clients use the previously valid URL for the private Insight server. If the Server URL has never been configured and you enter an invalid URL, clients use the default Symantec Insight server.

At the next heartbeat, your clients start to use the specified private server for reputation queries.

[How Symantec Endpoint Protection uses Symantec Insight to make decisions about files](#)

[Configuring client groups to use private servers for reputation queries and submissions](#)

## **Configuring client groups to use private servers for reputation queries and submissions**

You can direct client reputation queries (Insight lookups) from a group to a private intranet server. The private server can be the Symantec Endpoint Detection and Response appliance or the Symantec Insight for Private Clouds server that you purchase and install separately in your network.

**The following are the private server options for groups:**

- Symantec Endpoint Detection and Response  
Symantec EDR servers gather data about client detections and provide forensic analysis. When you use a Symantec EDR server, Symantec Endpoint Protection sends all reputation queries (lookups) and most types of client submissions to Symantec EDR. Symantec EDR then sends the queries or submissions to Symantec. Note that Symantec EDR receives antivirus, SONAR, and IPS submissions, but it does not receive file reputation submissions. Symantec Endpoint Protection always sends file reputation submissions directly to Symantec.
- Symantec Insight for Private Clouds  
This option redirects the reputation queries from clients in the group to a private Insight server. The private Insight server stores a copy of Symantec's Insight reputation database. The private Insight server handles the reputation queries rather than Symantec's Insight server. When you use a private Insight server, clients continue to send submissions about detections to Symantec. Typically, you use a private Insight server in a dark network, which is a network that is disconnected from the Internet. In that case, Symantec cannot receive any client submissions.

[Understanding server data collection and client submissions and their importance to the security of your network](#)

You can also copy the private server configuration to other client groups.

You can specify multiple private servers to load balance network traffic. You can also specify multiple groups of servers to manage failover.

When you choose to enable an EDR server, the EDR connection status appears in the client user interface as well as the management console logs and reports. To communicate with the EDR server, the Symantec Endpoint Protection client must at a minimum run Virus and Spyware Protection.

---

To configure client groups to use a private server

1. In the console, go to **Clients** and select the group that should use the private server list.
2. On the **Policies** tab, click **External Communications Settings**
3. On the **Private Cloud** tab, click **Enable private servers to manage my data**.
4. Depending on which type of server you use, click **Use an Advanced Threat Protection server for Insight lookups and submissions** or **Use a private Insight server for Insight lookups**.

You should not mix server types in the priority list.

5. Click **Use Symantec servers when private servers are not available** if you want clients to use Symantec servers for reputation queries and client antivirus and SONAR submissions.

Clients always send file reputation submissions to Symantec.

6. Under **Private Servers**, click **Add > New Server**.
7. In the **Add Private Server** dialog, select the protocol and then enter the host name for the URL.
8. Specify the port number for the server.
9. To add a priority group, click **Add > New Group**.
10. To apply the settings to additional client groups, click **Copy settings**. Select the groups and locations, and then click **OK**.

## Customizing virus and spyware scans

You can customize options for administrator-defined scans (scheduled and on-demand scans) that run on the devices in your environment. You can also customize options for Auto-Protect.

**Table 111: Customizing virus and spyware scans on Windows computers**

Task	Description
Customize Auto-Protect settings	<p>You can customize Auto-Protect in many ways, including the configuration for the following settings:</p> <ul style="list-style-type: none"><li>• The types of files that Auto-Protect scans</li><li>• The actions that Auto-Protect takes when it makes a detection</li><li>• The user notifications for Auto-Protect detections</li></ul> <p>You can also enable the <b>Scan Results</b> dialog for Auto-Protect scans of the file system.</p> <p><a href="#">Customizing Auto-Protect for Windows clients</a></p> <p><a href="#">Customizing Auto-Protect for email scans on Windows computers</a></p>
Customize administrator-defined scans	<p>You can customize the following types of options for scheduled and on-demand scans.</p> <ul style="list-style-type: none"><li>• Compressed files</li><li>• Tuning options</li><li>• Advanced schedule options</li><li>• User notifications about detections</li></ul> <p><a href="#">Customizing administrator-defined scans for clients that run on Windows computers</a></p> <p>You can also customize scan actions.</p>
Adjust ELAM settings	<p>You might want to enable or disable Symantec Endpoint Protection early launch anti-malware (ELAM) detection if you think ELAM is affecting your computers' performance. Or you might want to override the default detection setting if you get many false positive ELAM detections.</p> <p><a href="#">Managing early launch anti-malware (ELAM) detections</a></p>

Task	Description
Adjust Download Insight settings	You might want to adjust the malicious file sensitivity to increase or decrease the number of detections. You can also modify actions for detections and user notifications for detections. <a href="#">Customizing Download Insight settings</a>
Customize scan actions	You can change the action that Symantec Endpoint Protection takes when it makes a detection. <a href="#">Changing the action that Symantec Endpoint Protection takes when it makes a detection</a>
Customize global scan settings	You might want to customize global scan settings to increase or decrease the protection on your client computers. <a href="#">Modifying global scan settings</a> <a href="#">Global Scan Options</a>
Customize miscellaneous options for Virus and Spyware Protection	You can specify the types of risk events that clients send to Symantec Endpoint Protection Manager. <a href="#">Modifying log handling and notification settings on Windows computers</a>

**Table 112: Customizing virus and spyware scans on Mac computers**

Task	Description
Customize Auto-Protect	You can customize Auto-Protect settings for the clients that run on Mac computers. <a href="#">Customizing Auto-Protect for Mac clients</a>
Customize administrator-defined scans	You can customize common settings and notifications as well as scan priority. You can also enable a warning to alert the user when definitions are out-of-date. <a href="#">Customizing administrator-defined scans for clients that run on Mac computers</a>
Customize global scan options	You can specify the files or folders that you want Auto-Protect, scheduled scans, and manual scans to scan. <a href="#">Modifying global scan settings</a> <a href="#">Mac Global Scan Options</a>

**Table 113: Customizing virus and spyware scans on Linux computers**

Task	Description
Customize Auto-Protect settings	You can customize Auto-Protect in many ways, including the configuration for the following settings: <ul style="list-style-type: none"> <li>The types of files that Auto-Protect scans</li> <li>The actions that Auto-Protect takes when it makes a detection As of 14.3 RU1, configuring the actions for detections is deprecated for the Linux client.</li> <li>The user notifications for Auto-Protect detections</li> </ul> You can also enable or disable the <b>Scan Results</b> dialog for Auto-Protect scans of the file system. <a href="#">Customizing Auto-Protect for Linux clients</a>
Customize administrator-defined scans	You can customize the following types of options for scheduled and on-demand scans. <ul style="list-style-type: none"> <li>File and folder types</li> <li>Compressed files</li> <li>Security risks</li> <li>Scheduling options</li> <li>Actions for detections As of 14.3 RU1, configuring the actions for detections is deprecated for the Linux client.</li> <li>User notifications</li> </ul>
Customize scan actions (deprecated as of 14.3 RU1)	You can change the action that Symantec Endpoint Protection takes when it makes a detection. <a href="#">Changing the action that Symantec Endpoint Protection takes when it makes a detection</a>

Task	Description
Customize global scan options (available as of 14.3 RU3)	You can customize settings that apply to all virus and spyware scans that run on your Linux clients. <a href="#">Modifying global scan settings</a> <a href="#">Linux Global Scan Options</a>
Customize miscellaneous options for Virus and Spyware Protection (deprecated as of 14.3 RU1)	You can specify the types of risk events that clients send to Symantec Endpoint Protection Manager. <a href="#">Modifying log handling settings on Linux computers</a>

[Managing scans on client computers](#)

## Customizing the virus and spyware scans that run on Mac computers

You can customize options for administrator-defined scans (scheduled and on-demand scans) that run on Mac computers. You can also customize options for Auto-Protect.

**Table 114: Customizing virus and spyware scans on Mac computers**

Task	Description
Customize Auto-Protect	You can customize Auto-Protect settings for the clients that run on Mac computers. <a href="#">Customizing Auto-Protect for Mac clients</a>
Customize administrator-defined scans	You can customize common settings and notifications as well as scan priority. You can also enable a warning to alert the user when definitions are out-of-date. <a href="#">Customizing administrator-defined scans for clients that run on Mac computers</a>
Customize global scan options	You can specify the files or folders that you want Auto-Protect, scheduled scans, and manual scans to scan. <a href="#">Modifying global scan settings</a>

## Customizing the virus and spyware scans that run on Linux computers

You can customize options for administrator-defined scans (scheduled and on-demand scans) that run on Linux computers. You can also customize options for Auto-Protect.

**Table 115: Customizing virus and spyware scans on Linux computers**

Task	Description
Customize Auto-Protect settings	You can customize Auto-Protect in many ways, including the configuration for the following settings: <ul style="list-style-type: none"><li>• The types of files that Auto-Protect scans</li><li>• The actions that Auto-Protect takes when it makes a detection</li></ul> As of 14.3 RU1, configuring the actions for detections is deprecated for the Linux client. <ul style="list-style-type: none"><li>• The user notifications for Auto-Protect detections</li></ul> You can also enable or disable the <b>Scan Results</b> dialog for Auto-Protect scans of the file system. <a href="#">Customizing Auto-Protect for Linux clients</a>
Customize administrator-defined scans	You can customize the following types of options for scheduled and on-demand scans. <ul style="list-style-type: none"><li>• File and folder types</li><li>• Compressed files</li><li>• Security risks</li><li>• Scheduling options</li><li>• Actions for detections</li></ul> As of 14.3 RU1, configuring the actions for detections is deprecated for the Linux client. <ul style="list-style-type: none"><li>• User notifications</li></ul>
Customize scan actions (deprecated as of 14.3 RU1)	You can change the action that Symantec Endpoint Protection takes when it makes a detection. <a href="#">Changing the action that Symantec Endpoint Protection takes when it makes a detection</a>
Customize global scan options (available as of 14.3 RU3)	You can customize global settings for the scans that run on your Linux clients. <a href="#">Modifying global scan settings</a>
Customize miscellaneous options for Virus and Spyware Protection (deprecated as of 14.3 RU1)	You can specify the types of risk events that clients send to Symantec Endpoint Protection Manager. <a href="#">Modifying log handling settings on Linux computers</a>

## Customizing Auto-Protect for Windows clients

You might want to customize Auto-Protect settings for Windows clients.

To configure Auto-Protect for Windows clients

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Windows Settings**, under **Protection Technology**, click **Auto-Protect**.
3. On the **Scan Details** tab, make sure that **Enable Auto-Protect** is checked.

### WARNING

If you disable Auto-Protect, Download Insight cannot function even if it is enabled.

4. Under **Scanning**, under **File types**, select one of the following options:
  - **Scan all files**  
This option is the default and is the most secure option.
  - **Scan only selected extensions**  
You can improve scan performance by selecting this option, however, you might decrease the protection on your computer.

- 
5. Under **Additional options**, check or uncheck **Scan for security risks**.
  6. Click **Advanced Scanning and Monitoring** to change options for the actions that trigger Auto-Protect scans and how Auto-Protect handles scans of floppy disks.
  7. Click **OK**.
  8. Under **Network Settings**, check or uncheck **Scan files on remote computers** to enable or disable Auto-Protect scans of network files.

By default, Auto-Protect scans files on remote computers only when the files are executed.

You might want to disable network scanning to improve scan and computer performance.
  9. When file scans on remote computers is enabled, click **Network Settings** to modify network scanning options.
  10. In the **Network Settings** dialog box, do any of the following actions:
    - Enable or disable Auto-Protect to trust files on the remote computers that run Auto-Protect.
    - Configure network cache options for Auto-Protect scans.
  11. Click **OK**.
  12. On the **Actions** tab, set any of the options.

[Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)

You can also set remediation options for Auto-Protect.
  13. On the **Notifications** tab, set any of the notification options.

[Managing the virus and spyware notifications that appear on client computers](#)
  14. On the **Advanced** tab, set any of the following options:
    - **Startup and shutdown**
    - **Reload options**
  15. Under **Additional Options**, click **File Cache** or **Risk Tracer**.
  16. Configure the file cache or Risk Tracer settings, and then click **OK**.
  17. If you are finished with the configuration for this policy, click **OK**.

[Customizing the virus and spyware scans that run on Windows computers](#)

[Managing scans on client computers](#)

## Customizing Auto-Protect for Mac clients

You might want to customize Auto-Protect settings for the clients that run on Mac computers.

To customize Auto-Protect for Mac clients

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Mac Settings**, under **Protection Technology**, click **Auto-Protect and SONAR**.
3. At the top of the **Scan Details** tab, click the lock icon to lock or unlock all settings.
4. Check or uncheck any of the following options:
  - **Enable Auto-Protect**
  - **Automatically repair infected files**
  - **Quarantine files that cannot be repaired**
  - **Scan compressed files**

- 
- Under **General Scan Details**, specify the files that Auto-Protect scans.

**NOTE**

To exclude files from the scan, you must select **Scan everywhere except in specified folders**, and then add an Exceptions policy to specify the files to exclude.

[Excluding a file or a folder from scans](#)

- Under **Scan Mounted Disk Details**, check or uncheck any of the available options.
- Under **Suspicious Behavior Detection**, check or uncheck **Enable Suspicious Behavior Detection**.  
This option is available as of version 14.3 RU1.
- On the **Notifications** tab, set any of the notification options, and then click **OK**.

[Customizing the virus and spyware scans that run on Mac computers](#)

[Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)

[Managing the virus and spyware notifications that appear on client computers](#)

## Customizing Auto-Protect for Linux clients

You might want to customize Auto-Protect settings for the clients that run on Linux computers.

**NOTE**

As of 14.3 RU1, configuring the options on the **Actions** tab, **Notifications** tab, and **Advanced** tab (steps 9, 10, and 11) is deprecated for the Linux client.

To customize Auto-Protect for Linux clients

- In the console, open a Virus and Spyware Protection policy.
- Under **Linux Settings**, under **Protection Technology**, click **Auto-Protect**.
- On the **Scan Details** tab, check or uncheck **Enable Auto-Protect**.
- Under **Scanning**, under **File types**, click one of the following options:
  - **Scan all files**  
This option is the default and is the most secure option.
  - **Scan only selected extensions**  
You can improve scan performance by selecting this option, however, you might decrease the protection on your computer.  
(Not available as of 14.3 RU1)
- Under **Additional options**, check or uncheck **Scan for security risks**.
- Click **Advanced Scanning and Monitoring** to change options for the actions that trigger Auto-Protect scans and how Auto-Protect handles scans of compressed files.
- Click **OK**.
- Under **Network Settings**, check or uncheck **Scan files on remote computers** to enable or disable Auto-Protect scans of network files.  
  
By default, Auto-Protect scans files on remote computers only when the files are executed.  
  
You might want to disable network scanning to improve scan and computer performance.
- On the **Actions** tab, set any of the options.

[Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)

---

You can also set remediation options for Auto-Protect.

10. On the **Notifications** tab, set any of the notification options.

[Managing the virus and spyware notifications that appear on client computers](#)

11. On the **Advanced** tab, check or uncheck **Enable the cache**.

Set a cache size or accept the default.

12. Click **OK**.

[Customizing the virus and spyware scans that run on Linux computers](#)

[Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)

[Managing the virus and spyware notifications that appear on client computers](#)

## Customizing Auto-Protect for email scans on Windows computers

You can customize Auto-Protect for email scans on Windows computers.

To customize Auto-Protect for email scans on Windows computers

1. In the console, open a Virus and Spyware Protection policy.

2. Under **Windows Settings**, select one of the following options:

- **Microsoft Outlook Auto-Protect**
- **Internet Email Auto-Protect\***
- **Lotus Notes Auto-Protect\***

\* Only available for client versions earlier than 14.2 RU1.

3. On the **Scan Details** tab, check or uncheck **Enable Internet Email Auto-Protect**.

4. Under **Scanning**, under **File types**, select one of the following options:

- **Scan all files**

This option is the default and most secure option.

- **Scan only selected extensions**

You can improve scan performance by selecting this option, however, you might decrease the protection on your computer.

5. Check or uncheck **Scan files inside compressed files**.

6. On the **Actions** tab, set any of the options.

[Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)

7. On the **Notifications** tab, under **Notifications**, check or uncheck **Display a notification message on the infected computer**. You can also customize the message.

8. Under **Email Notifications**, check or uncheck any of the following options:

- **Insert a warning into the email message**
- **Send email to the sender**
- **Send email to others**

You can customize the message text and include a warning. For Internet Email Auto-Protect you must also specify the mail server.



- 
9. For Internet Email Auto-Protect only, on the **Advanced** tab, under **Encrypted Connections**, enable or disable encrypted POP3 or SMTP connections.
  10. Under **Mass Mailing Worm Heuristics**, check or uncheck **Outbound worm heuristics**.
  11. If you are finished with the configuration for this policy, click **OK**.

[Customizing the virus and spyware scans that run on Windows computers](#)

[Managing the virus and spyware notifications that appear on client computers](#)

## Customizing administrator-defined scans for clients that run on Windows computers

You might want to customize scheduled or on-demand scans for the clients that run on Windows computers. You can set options for scans of compressed files and optimize the scan for computer or scan performance.

To customize an administrator-defined scan for the clients that run on Windows computers

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Windows Settings**, click **Administrator-defined scans**.
3. Do one of the following actions:
  - Under **Scheduled Scans**, select the scheduled scan that you want to customize, or create a new scheduled scan.
  - Under **Administrator On-demand Scan**, click **Edit**.
4. On the **Scan Details** tab, select **Advanced Scanning Options**:
  - On the **Compressed Files** tab, you can reduce the number of levels to scan compressed files. If you reduce the number of levels, you might improve client computer performance.
  - On the **Tuning** tab, change the tuning level for the best client computer performance or the best scan performance.Click **OK** to save changes.
5. For scheduled scans only, on the **Schedule** tab, set any of the following options:
  - **Scan Duration**  
You can set how long the scan runs before it pauses and waits until the client computer is idle. You can also randomize scan start time.
  - **Missed Scheduled Scans**  
You can specify a retry interval for missed scans.
6. On the **Actions** tab, change any detection actions.

[Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)

7. On the **Notifications** tab, enable or disable a notification that appears on client computers when the scan makes a detection.

[Managing the virus and spyware notifications that appear on client computers](#)

8. Click **OK**.

[Customizing the virus and spyware scans that run on Windows computers](#)

[Setting up scheduled scans that run on Windows computers](#)

---

## Customizing administrator-defined scans for clients that run on Mac computers

You customize scheduled scans and on-demand scans separately. Some of the options are different.

1. To customize a scheduled scan that runs on Mac computers, in the console, open a Virus and Spyware Protection policy.
2. Under **Mac Settings**, select **Administrator-Defined Scans**.
3. Under **Scheduled Scans**, select the scheduled scan that you want to customize, or create a new scheduled scan.  
For a new scan, you can create a new scan manually, or create a scheduled scan from a template.
4. On the **Scan Details** tab, under **Scan drives and folders**, select the items that you want to scan.
5. You can also enable or disable idle-time scans. Enabling the option improves computer performance; disabling the option improves scan performance.
6. Click **OK**.

Edit the scan details for any other scan that is included in this policy.

7. On the **Notifications** tab, enable or disable notification messages about scan detections. The setting applies to all scheduled scans that you include in this policy.
8. On the **Common Settings** tab, set any of the following options:
  - **Scan Options**
  - **Actions**
  - **Alerts**

These options apply to all scheduled scans that you include in this policy.

9. Click **OK**.
10. To customize the on-demand scans that run on Mac computers, on the Virus and Spyware Protection Policy page, under **Mac Settings**, select **Administrator-Defined Scans**.
11. Under **Administrator On-demand Scan**, click **Edit**.
12. On the **Scan Details** tab, under **Scan drives and folders**, select the items that you want to scan.  
You can also specify actions for scan detections and enable or disables scans of compressed files.
13. On the **Notifications** tab, enable or disable notifications for detections.  
You can also specify the message that appears on the client.
14. Click **OK**.

[Customizing the virus and spyware scans that run on Mac computers](#)

[Setting up scheduled scans that run on Mac computers](#)

[Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)

[Managing the virus and spyware notifications that appear on client computers](#)

## Customizing administrator-defined scans for clients that run on Linux computers

You might want to customize scheduled or on-demand scans for the clients that run on Linux computers. You can set options for scans of compressed files and optimize the scan for computer or scan performance.

To customize an administrator-defined scan for the clients that run on Linux computers

- 
1. In the console, open a Virus and Spyware Protection policy.
  2. Under **Linux Settings**, click **Administrator-defined scans**.
  3. Do one of the following actions:
    - Under **Scheduled Scans**, select the scheduled scan that you want to customize, or create a new scheduled scan.
    - Under **Administrator On-demand Scan**, click **Edit**.
  4. On the **Scan Details** tab, check **Scan all folders** or specify the particular folders you want to scan.
  5. Click **Scan all files** or **Scan only selected extensions** and specify the extensions you want to scan.  
As of 14.3 RU1, **Scan only selected extensions** option is not available.
  6. On the **Scan files inside compressed files** choice, you can reduce the number of levels to scan compressed files. If you reduce the number of levels, you might improve client computer performance.
  7. Check or uncheck **Scan for security risks**.
  8. For scheduled scans only, on the **Schedule** tab, set any of the following options:
    - **Scanning schedule**  
You can set how often the scan runs, on a daily, weekly, or monthly basis.
    - **Missed Scheduled Scans**  
You can specify a retry interval for missed scans.
  9. On the **Actions** tab, change any detection actions.  
[Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)  
As of 14.3 RU1, configuring the actions for detections is deprecated for the Linux client.
  10. On the **Notifications** tab, enable or disable a notification that appears on client computers when the scan makes a detection.  
[Managing the virus and spyware notifications that appear on client computers](#)
  11. Click **OK**.

[Customizing the virus and spyware scans that run on Linux computers](#)

[Setting up scheduled scans that run on Linux computers](#)

[Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)

[Managing the virus and spyware notifications that appear on client computers](#)

## Randomizing scans to improve computer performance in virtualized environments on Windows clients

You can randomize scheduled scans to improve performance on Windows client computers. Randomization is important in virtualized environments.

For example, you might schedule scans to run at 8:00 P.M. If you select a four-hour time interval, scans on client computers start at a randomized time between 8:00 P.M. and 12:00 A.M.

To randomize scans to improve computer performance in virtualized environments

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Windows Settings**, click **Administrator-defined Scans**.
3. Create a new scheduled scan or select an existing scheduled scan to edit.
4. In the **Add Scheduled Scan** or **Edit Scheduled Scan** dialog box, click the **Schedule** tab.
5. Under **Scanning Schedule**, select how often the scan should run.
6. Under **Scan Duration**, check **Scan for up to** and select the number of hours. The number of hours controls the time interval during which scans are randomized.
7. Make sure that you enable **Randomize scan start time within this period (recommended in VMs)**.
8. Click **OK**.
9. Make sure that you apply the policy to the group that includes the computers that run Virtual Machines.

[Adjusting scans to improve computer performance](#)

[Setting up scheduled scans that run on Windows computers](#)

## Modifying global scan settings

You can customize settings that apply to all virus and spyware scans that run on your client computers. You might want to modify these options to increase security on your client computers.

### NOTE

If you increase the protection on your client computers by modifying these options, you might affect client computer performance.

[Managing scans on client computers](#)

[Customizing virus and spyware scans](#)

### To modify global scan settings

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Windows Settings**, **Mac Settings**, or **Linux Settings**, click **Global Scan Options**.
3. Configure the options for any of the following operating systems:

Windows	<a href="#">Global Scan Options</a>
Mac	<a href="#">Mac Global Scan Options</a>
Linux	(as of 14.3 RU3) <a href="#">Linux Global Scan Options</a>

Insight	Insight allows scans to skip the files that Symantec trusts as good (more secure) or that the community trusts as good (less secure).
Bloodhound	Bloodhound isolates and locates the logical regions of a file to detect a high percentage of unknown viruses. Bloodhound then analyzes the program logic for virus-like behavior. You can specify the level of sensitivity for detection.
Password for mapped network drives	Specifies whether or not clients prompt users for a password when the client scans network drives.

- 
- Click **OK**.

## Modifying log handling and notification settings on Windows computers

Each Virus and Spyware Protection policy includes the options that apply to all virus and spyware scans that run on Windows client computers.

**You can set the following options:**

- Specify a default URL that Symantec Endpoint Protection uses when it repairs a security risk that changed a browser home page.
- Specify Risk log handling options.
- Warn users when definitions are out-of-date or missing.
- Exclude virtual images from Auto-Protect or administrator-defined scans.

To modify log handling and notification settings on Windows computers

- In the console, open a Virus and Spyware Protection policy.
- Under **Windows Settings**, click **Miscellaneous**.

Specify options for **Internet Browser Protection**.

- On the **Log Handling** tab, set options for event filtering, log retention, and log aggregation.
- On the **Notifications** tab, configure global notifications.

[Customizing the virus and spyware scans that run on Windows computers](#)

- Click **OK**.

[Managing the virus and spyware notifications that appear on client computers](#)

## Modifying log handling settings on Linux computers

Each Virus and Spyware Protection policy includes log handling settings that apply to all virus and spyware scans that run on Linux client computers.

As of 14.3 RU1, modifying log handling settings is deprecated for the Linux client.

To log handling settings Linux computers

- In the console, open a Virus and Spyware Protection policy.
- Under **Linux Settings**, click **Miscellaneous**.
- On the **Log Handling** tab, set options for event filtering, log retention, and log aggregation.

[Viewing logs](#)

## Customizing Download Insight settings

You might want to customize Download Insight settings to decrease false positive detections on client computers. You can change how sensitive Download Insight is to the file reputation data that it uses to characterize malicious files. You can also change the notifications that Download Insight displays on client computers when it makes a detection.

[Customizing the virus and spyware scans that run on Windows computers](#)

[Managing Download Insight detections](#)

To customize Download Insight settings

- 
1. In the console, open a Virus and Spyware Protection policy and select **Download Protection**.
  2. On the **Download Insight** tab, make sure that **Enable Download Insight to detect potential risks in downloaded files based on file reputation** is checked.  
If Auto-Protect is disabled, Download Insight cannot function even if it is enabled.
  3. Move the slider for malicious file sensitivity to the appropriate level.  
If you set the level higher, Download Insight detects more files as malicious and fewer files as unproven. Higher settings, however, return more false positives.
  4. Check the following options to use as additional criteria for examining unproven files:
    - **Files with x or fewer users**
    - **Files known by users for x or fewer days**When unproven files meet these criteria, Download Insight detects the files as malicious.
  5. Make sure that **Automatically trust any file downloaded from a trusted Internet or intranet site** is checked.
  6. On the **Actions** tab, under **Malicious Files**, specify a first action and a second action.
  7. Under **Unproven Files**, specify the action.
  8. On the **Notifications** tab, specify whether or not to display a message on client computers when Download Insight makes a detection.  
You can also customize the text of a warning message that appears when a user allows a file that Download Insight detects.
  9. Click **OK**.

## Changing the action that Symantec Endpoint Protection takes when it makes a detection

You can configure the action or actions that scans should take when they make a detection. Each scan has its own set of actions, such as Clean, Quarantine, Delete, or Leave alone (log only).

On Windows clients and Linux clients, each detection category can be configured with a first action and a second action in case the first action is not possible.

As of 14.3 RU1, configuring the actions for detections is deprecated for the Linux client.

**By default, Symantec Endpoint Protection tries to clean a file that a virus infected. If Symantec Endpoint Protection cannot clean a file, it performs the following actions:**

- Moves the file to the Quarantine on the infected computer and denies any access to the file.
- Logs the event.

By default, Symantec Endpoint Protection moves any files that security risks infect into the Quarantine.

If you set the action to log only, by default if users create or save infected files, Symantec Endpoint Protection deletes them.

On Windows computers, you can also configure remediation actions for administrator scans, on-demand scans, and Auto-Protect scans of the file system.

You can lock actions so that users cannot change the action on the client computers that use this policy.

---

## WARNING

For security risks, use the Delete action with caution. In some cases, deleting security risks causes applications to lose functionality. If you configure the client to delete the files that security risks affect, it cannot restore the files.

To back up the files that security risks affect, use the Quarantine action instead.

1. **Option 1:** To change the action that Symantec Endpoint Protection takes when it makes a detection on Windows or Linux clients, in the Virus and Spyware Protection policy, under **Windows Settings** or **Linux Settings**, select the scan (any Auto-Protect scan, administrator scan, or on-demand scan).

As of 14.3 RU1, configuring the actions for detections is deprecated for the Linux client.

2. On the **Actions** tab, under **Detection**, select a type of malware or security risk.

By default, each subcategory is automatically configured to use the actions that are set for the entire category.

## NOTE

On Windows clients, the categories change dynamically over time as Symantec gets new information about risks.

3. To configure actions for a subcategory only, do one of the following actions:

- Check **Override actions configured for Malware**, and then set the actions for that subcategory only.

## NOTE

There might be a single subcategory under a category, depending on how Symantec currently classifies risks. For example, under **Malware**, there might be a single subcategory called Viruses.

- Check **Override actions configured for Security Risks**, and then set the actions for that subcategory only.

4. Under **Actions for**, select the first and second actions that the client software takes when it detects that category of virus or security risk.

For security risks, use the Delete action with caution. In some cases, deleting security risks causes applications to lose functionality.

5. Repeat these steps for each category for which you want to set actions (viruses and security risks).
6. When you finish configuring this policy, click **OK**.
7. **Option 2:** To change the action that Symantec Endpoint Protection takes when it makes a detection on Mac clients, in the Virus and Spyware Protection policy, under **Mac Settings**, select **Administrator-Defined Scans**.
8. Do one of the following actions:
  - For scheduled scans, select the **Common Settings** tab.
  - For on-demand scans, on the **Scans** tab, under **Administrator On-demand Scan**, click **Edit**.
9. Under **Actions**, check either of the following options:
  - **Automatically repair infected files**
  - **Quarantine files that cannot be repaired**
10. For on-demand scans, click **OK**.
11. When you finish configuring this policy, click **OK**.

[Checking the scan action and rescanning the identified computers](#)

[Removing viruses and security risks](#)

---

## Allowing users to view scan progress and interact with scans on Windows computers

You can configure whether or not the scan progress dialog box appears on Windows client computers. If you allow the dialog box to appear on client computers, users are always allowed to pause or delay an administrator-defined scan.

When you allow users to view scan progress, a link appears in the main pages of the client UI to display scan progress for the currently running scan. A link to reschedule the next scheduled scan also appears.

**When you allow users to view scan progress, the following options appear in the main pages of the client UI:**

- When a scan runs, the message link **scan in progress** appears.  
The user can click the link to display the scan progress.
- A link to reschedule the next scheduled scan also appears.

You can allow users to stop a scan entirely. You can also configure options for how users pause or delay scans.

You can allow the user to perform the following scan actions:

Pause	When a user pauses a scan, the Scan Results dialog box remains open and waits for the user to either continue or abort the scan. If the computer is turned off, the paused scan does not continue.
Snooze	When a user snoozes a scheduled scan, the user has the option of snoozing the scan for one hour or three hours. The number of snoozes is configurable. When a scan snoozes, the Scan Results dialog box closes; it reappears when the snooze period ends and the scan resumes.
Stop	When a user stops a scan, the scan usually stops immediately. If a user stops a scan while the client software scans a compressed file, the scan does not stop immediately. In this case, the scan stops as soon as the compressed file has been scanned. A stopped scan does not restart.

A paused scan automatically restarts after a specified time interval elapses.

### NOTE

Users can stop a Power Eraser analysis but cannot pause or snooze it.

You can click Help for more information about the options that are used in this procedure.

To allow users to view scan progress and interact with scans on Windows computers

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Windows Settings**, click **Administrator-defined Scans**.
3. On the **Advanced** tab, under **Scan Progress Options**, click **Show scan progress** or **Show scan progress if risk detected**.
4. To automatically close the scan progress indicator after the scan completes, check **Close the scan progress window when done**.
5. Check **Allow user to stop scan**.
6. Click **Pause Options**.
7. In the **Scan Pause Options** dialog box, do any of the following actions:
  - To limit the time that a user may pause a scan, check **Limit the time the scan may be paused**, and then type a number of minutes. The range is 3 to 180.
  - To limit the number of times a user may delay (or snooze) a scan, in the **Maximum number of snooze opportunities** box, type a number between 1 and 8.
  - By default, a user can delay a scan for one hour. To change this limit to three hours, check **Allow users to snooze the scan for 3 hours**.



8. Click **OK**.

#### Managing scans on client computers

## Configuring Windows Security Center notifications to work with Symantec Endpoint Protection clients

You can use a Virus and Spyware Protection policy to configure Windows Security Center settings on your client computers that run Windows XP Service Pack 3.

#### Customizing administrator-defined scans for clients that run on Windows computers

##### NOTE

You can configure all the Windows Security Center options on your client computers that run Windows XP SP3 only. You can only configure the **Display a Windows Security Center message when definitions are outdated** option on Windows Vista and Windows 7 and later.

**Table 116: Options to configure how Windows Security Center works with the client**

Option	Description	When to use
<b>Disable Windows Security Center</b>	Lets you permanently or temporarily disable Windows Security Center on your client computers. <b>Available options:</b> <ul style="list-style-type: none"><li>• Never. Windows Security Center is always enabled on the client computer.</li><li>• Once. Windows Security Center is disabled only once. If a user enables it, it is not disabled again.</li><li>• Always. Windows Security Center is permanently disabled on the client computer. If a user enables it, it is immediately disabled.</li><li>• Restore. Windows Security Center is enabled if the Virus and Spyware Protection Policy previously disabled it.</li></ul>	Disable Windows Security Center permanently if you do not want your client users to receive the security alerts that it provides. Client users can still receive Symantec Endpoint Protection alerts. Enable Windows Security Center permanently if you want your client users to receive the security alerts that it provides. You can set Windows Security Center to display Symantec Endpoint Protection alerts.
<b>Display antivirus alerts within Windows Security Center</b>	Lets you set antivirus alerts from the Symantec Endpoint Protection client to appear in the Windows notification area.	Enable this setting if you want your users to receive Symantec Endpoint Protection alerts with other security alerts in the Windows notification area of their computers.
<b>Display a Windows Security Center message when definitions are outdated</b>	Lets you set the number of days after which Windows Security Center considers definitions to be outdated. By default, Windows Security Center sends this message after 30 days.	Set this option if you want Windows Security Center to notify your client users about outdated definitions more frequently than the default time (30 days). <b>Note:</b> On client computers, Symantec Endpoint Protection checks every 15 minutes to compare the out-of-date time, the date of the definitions, and the current date. Typically, no out-of-date status is reported to Windows Security Center because definitions are usually updated automatically. If you update definitions manually you might have to wait up to 15 minutes to view an accurate status in Windows Security Center.

To configure Windows Security Center to work with Symantec Endpoint Protection clients

- 
1. In the console, open a Virus and Spyware Protection policy.
  2. Under **Windows Settings**, click **Miscellaneous**.
  3. On the **Miscellaneous** tab, specify options for the Windows Security Center.
  4. Click **OK**.

## Submitting Symantec Endpoint Protection telemetry to improve your security

[Introduction](#)

[Purpose](#)

[Enabling telemetry collection](#)

[Frequently asked questions - What problems does TELEMETRY solve?](#)

[Performance, sizing, and deployment](#)

### Introduction

Telemetry, also known as submissions or data collection, collects information to improve the security posture of your network and improve the product experience. Telemetry broadly collects the following types of information:

- System environment, including hardware and software details
- Product errors and related events
- Effectiveness of the product configuration

The collected data is sent to Symantec.

#### NOTE

The data that Symantec telemetry collects may include pseudonymous elements that are not directly identifiable. Symantec neither needs nor seeks to use telemetry data to identify any individual user.

### Purpose

Symantec uses the information to analyze and improve product experience for customers.

- Symantec Support uses telemetry.
- Symantec uses telemetry for insights into the threat landscape and as part of the Risk Insight program.

### Enabling telemetry collection

Symantec collects telemetry data from both the management server and the Symantec Endpoint Protection client.

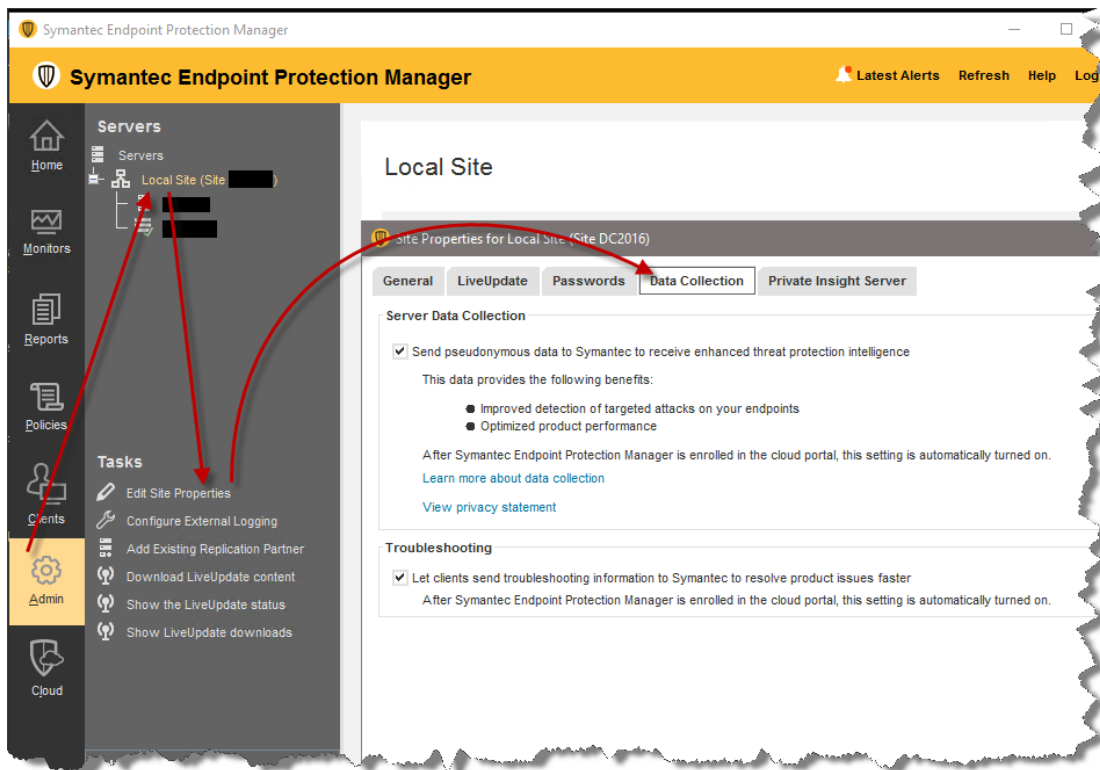
You might need to disable telemetry submissions, however, in response to network bandwidth issues or restrictions on data leaving the client. You can check the Client Activity log to view submissions activity and monitor your bandwidth usage.

To enable or disable management server telemetry collection

1. Enable or disable the **Send pseudonymous data to Symantec to receive enhanced threat protection intelligence** option for server data collection.
  - In the management console, go to **Admin > Servers > Local Site > Site Properties > Data Collection** and change the option.

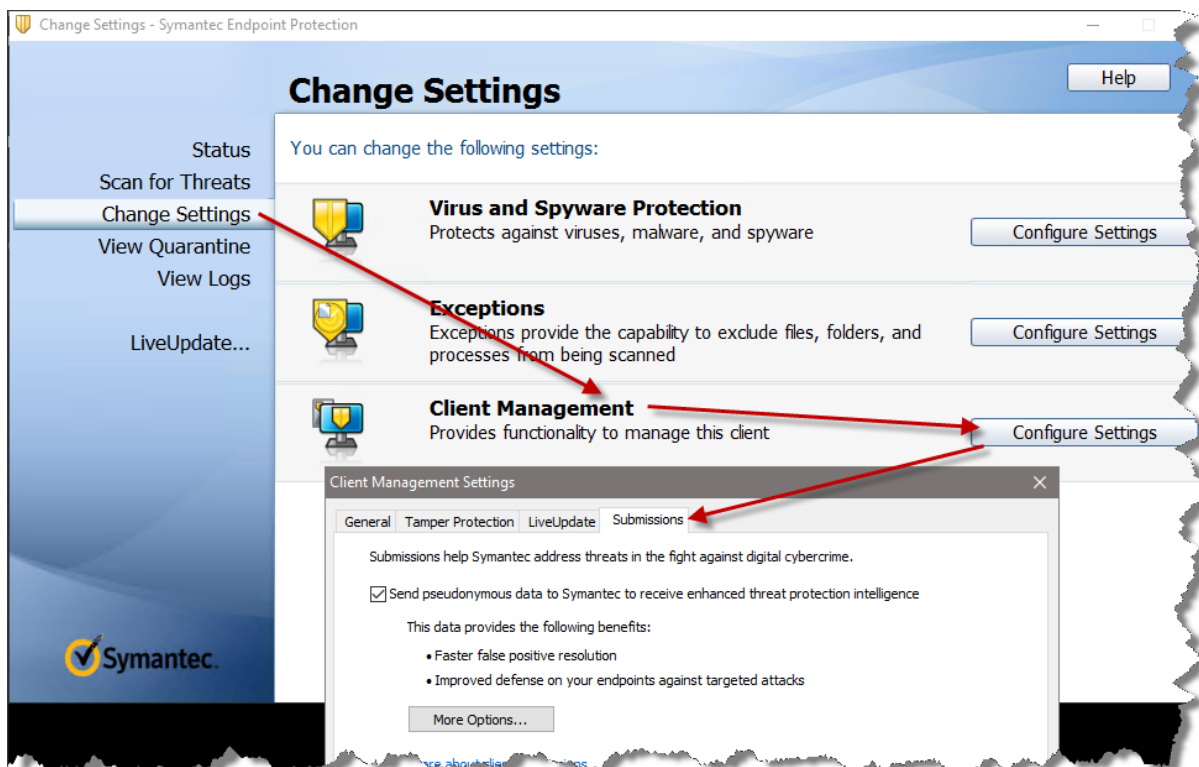
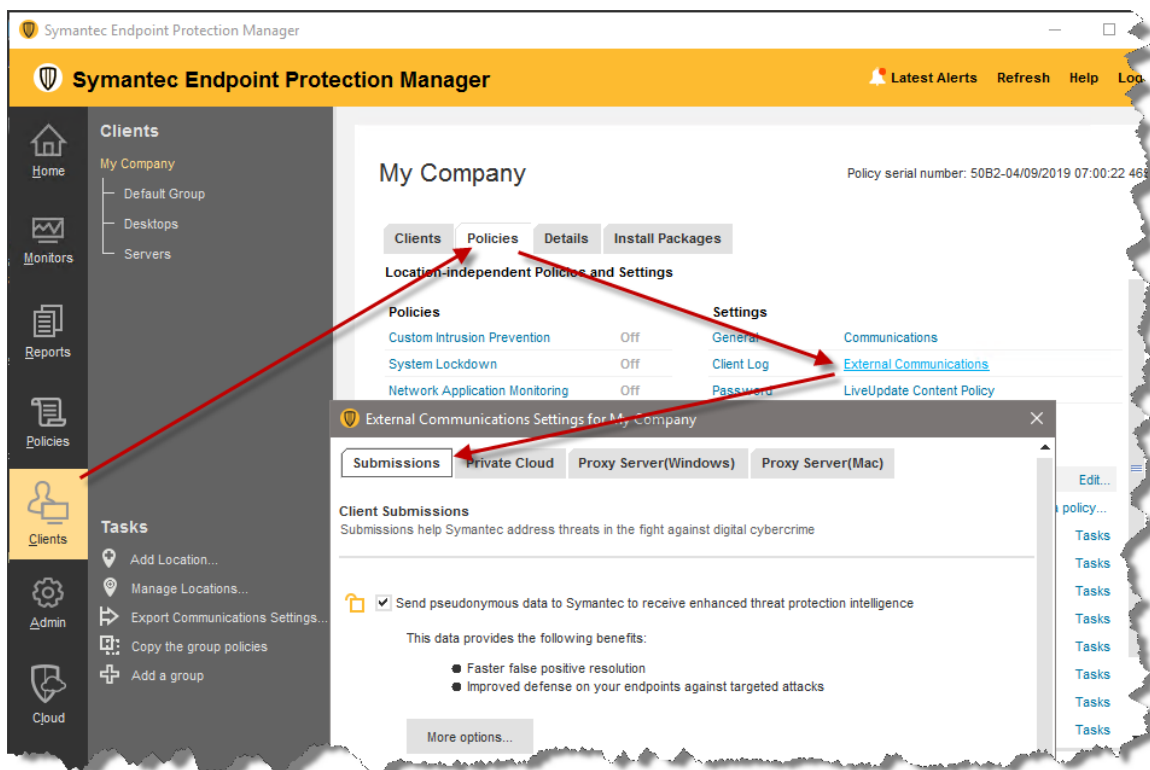
#### NOTE

During the installation of the Symantec Endpoint Protection Manager, you can also change the server data collection option.



To enable or disable client telemetry submissions

2. Enable or disable the **Send pseudonymous data to Symantec to receive enhanced threat protection intelligence** option for client submissions. You can change the option at the group level in the management console, or for a single client in the client user interface.
  - In the management console, go to **Clients > Policies** tab. In the **Settings** pane, select **External Communications Settings > Submissions**.
  - In the client user interface, go to **Change Settings > Client Management > Configure Settings > Submissions**.



Each client in the enterprise belongs to a group. A group has its own policy. In some cases, a group is configured to inherit the policy from its parent group. Since the client submissions are a group-wide setting, make sure that you apply the setting as necessary to all groups.

---

## NOTE

If you disable submissions and lock the setting, the user cannot configure clients in the group to send submissions. If you enable the option, select submission types and lock the setting, the user cannot disable submissions. If you do not lock the setting, the user can change the configuration, including the submission types in **More Options**.

Symantec recommends that you submit threat information to help Symantec provide the best threat protection.

## Frequently asked questions

### What types of information does Symantec Endpoint Protection collect?

#### [Privacy and Data Protection](#)

The following table describes the type of information that Symantec Endpoint Protection collects.

**Table 117: More details about the types of information that Symantec Endpoint Protection collects**

Type	More Details
Software configuration, product details and installation status	<p><b>Includes information about Virus and Spyware Protection policies:</b></p> <ul style="list-style-type: none"> <li>• <b>Bloodhound settings</b> Whether or not Bloodhound is enabled or disabled, and whether the level is automatic or aggressive. (<b>Virus and Spyware Protection policy &gt; Global Scan Options</b>)</li> <li>• <b>Download Insight settings</b> Whether Download Insight is enabled or disabled, and what the Download Insight settings are, including the sensitivity level and prevalence threshold. (<b>Virus and Spyware Protection policy &gt; Download Protection</b>)</li> <li>• <b>Auto-Protect settings</b> What overrides are configured for malware or security risks. (<b>Virus and Spyware Protection policy &gt; Auto-Protect</b>)</li> </ul> <p>Includes information about the top 20 groups with the most number of clients. For each group, the first location, typically the default location, is selected to send the information.</p> <p><b>Typically, the information includes:</b></p> <ul style="list-style-type: none"> <li>• Client mode: Whether the client uses server control, client control, mixed mode, or no data found</li> <li>• Push/pull mode: Whether the client gets or requests policies from the server</li> <li>• Application learning on or off</li> <li>• Heartbeat interval in minutes</li> <li>• Upload of critical events on or off</li> <li>• Download randomization on or off; randomization window in minutes</li> <li>• Whether the client uses last-used group settings or last-used group mode</li> <li>• Whether the client sends detection submissions and what type, such as antivirus detections, file reputation, or SONAR</li> <li>• Whether Host Integrity is enabled on the client</li> <li>• The number of domains.</li> <li>• The total number of groups in all domains, that is shown in approximations such as <b>&lt;1500</b>. More than 3,000 is sent as <b>&gt;= 3000</b></li> <li>• The maximum depth of group among all domains</li> <li>• The count of the total number of clients</li> <li>• The number of clients in computer mode</li> <li>• The number of clients in user mode</li> <li>• The number of clients in organizational unit (OU) groups</li> </ul>
License status, license entitlement information, license ID and license usage	N/A
Device name, type, OS version, language, location, browser type and version, IP address and ID	N/A
Device hardware, software and application inventory	The server database sends the aggregate information about the client hardware. The information includes CPU, RAM, and free disk space on the Symantec Endpoint Protection installation disk.

Type	More Details
Application and database access configurations, policy requirements and policy compliance status, and application exception and workflow failure logs	<p>Includes the number of rules for System Administrative log entries. Also sends the number of log entries as well as the number of days until the log entries expire for the following database logs:</p> <ul style="list-style-type: none"> <li>• System Administrative log</li> <li>• Client-Server Activity log</li> <li>• Audit log</li> <li>• System Server Activity log</li> </ul> <p>Includes any server replication failure events, such as replication failure or database versions that do not match.</p>
Information associated with possible threats including: client security event information, IP address, User ID, path, device information such as device name and status, files downloaded, file actions	N/A
File and application reputation information including file downloads, actions and executing application information, and malware submissions	<p><b>File reputation data is information about the files that are detected based on their reputation.</b></p> <ul style="list-style-type: none"> <li>• These submissions contribute to the Symantec Insight reputation database and helps protect your computers from new and emerging risks.</li> </ul> <p>The information includes file hash, client IP hash, IP address from where the file was downloaded, file size, and reputation score of the file.</p>
Application exception and workflow failure logs	N/A
Personal information provided during configuration of the Service or any other subsequent service call	N/A
Licensing information such as name, version, language and licensing entitlement data	N/A
Usage of protection technologies included in SEP	<p>Includes information about the top 20 groups with the most number of clients. For each group, the first location, typically the default location, is selected to send the information.</p> <p>The information includes:</p> <ul style="list-style-type: none"> <li>• The number of clients that have a particular protection technology enabled or disabled.</li> <li>• The number of and type (such as <b>Quarantine</b>, <b>Log only</b>, <b>Clean</b>, etc.) of the first and second actions for detections by the protection technologies that are enabled.</li> </ul> <p>Symantec Endpoint Protection Manager sends the number of shared policies of each type in its database, which is equal to the number of default policies plus the number of custom policies. The information includes:</p> <ul style="list-style-type: none"> <li>• The number of domains</li> <li>• The number of each of the following shared policies: <ul style="list-style-type: none"> <li>– Virus and Spyware Protection policies</li> <li>– Firewall policies</li> <li>– Intrusion Prevention policies</li> <li>– Application and Device Control policies</li> <li>– LiveUpdate policies</li> <li>– Host Integrity policies</li> </ul> </li> <li>• The number of custom intrusion prevention signatures</li> </ul>

Type	More Details
Information that describes the configuration of SEP, such as operating system information, server hardware and software configuration specifics, CPU name, memory size, software version and features for installed packages	<p><b>Includes server information such as:</b></p> <ul style="list-style-type: none"> <li>• Number of replication partners</li> <li>• Whether log data is replicated</li> <li>• Whether content data is replicated</li> </ul> <p>Includes the Linux operating system type and kernel versions, plus a count of the number of clients with this configuration.</p> <p>Includes the aggregation information in the Symantec Endpoint Protection Manager database about Symantec Endpoint Protection client operational state, including counts of the following:</p> <ul style="list-style-type: none"> <li>• Total clients</li> <li>• Reduced-size clients</li> <li>• Standard-size clients</li> <li>• EWF-enabled clients</li> <li>• FBWF-enabled clients</li> <li>• UWF-enabled clients</li> <li>• Microsoft hypervisor clients</li> <li>• VMware hypervisor clients</li> <li>• Citrix hypervisor clients</li> <li>• Unknown hypervisor clients</li> </ul> <p>Sends the approximate number of LiveUpdate revisions, for example &lt;30.</p>
Information on potential security risks, portable executable files and files with executable content that are identified as malware which may contain personal information, including information on the actions taken by such files at the time of installation	<ul style="list-style-type: none"> <li>• Antivirus detections (Windows and Mac only) Information about virus and spyware scan detections. The type of information that clients submit includes file hash, client IP hash, antivirus signatures, attacker URL, etc.</li> <li>• Antivirus advanced heuristic detections (Windows only) Information about the potential threats that Bloodhound and other virus and spyware scan heuristics detect. These detections are silent and do not appear in the Risk log. Information about these detections is used for statistical analysis.</li> <li>• SONAR detections (Windows only) Information about the threats that SONAR detects, which include high or low risk detections, system change events, and suspicious behavior from trusted applications.</li> </ul> <p><b>Also includes process data such as:</b></p> <ul style="list-style-type: none"> <li>• SONAR heuristic detections (Windows only) are silent and do not appear in the Risk log. This information is used for statistical analysis. The type of information that clients submit typically includes attributes of the detection such as the following: <ul style="list-style-type: none"> <li>– Hidden processes</li> <li>– Small footprint processes</li> <li>– Keystroke logging or screen capture behavior</li> <li>– Disabling of security product behavior</li> <li>– Date and timestamps of detection</li> </ul> </li> </ul>
Information related to network activity including URLs accessed and aggregate information on network connections (e.g., hostname, IP addresses and statistical info on a network connection)	<p><b>Includes the following:</b></p> <ul style="list-style-type: none"> <li>• Network detection events (Windows and Mac only) Information about detections by the IPS engine (intrusion prevention). The information that clients submit includes client IP hash, attacker URL, detection timestamp, attacker IP address, IPS signature, etc.</li> <li>• Browser detection events (Windows only) All URLs typed in the browser address bar, clicked on, or connected to for downloading. Clients also send metadata about the following: <ul style="list-style-type: none"> <li>– Each network connection, including IP addresses, port numbers, host names, applications initiating connections, protocols, connection time, number of bytes per connection.</li> <li>– All file transfer activities between devices, including device identification, time of the transfer, protocol, file attributes (type, name, path, size), and SHA-256 of the content.</li> </ul> </li> </ul>



Type	More Details
Status information regarding installation and operation of SEP, which may contain personal information only if such information is included in the name or file folder encountered by SEP at the time of installation or error, and indicates to Symantec whether installation of SEP was successfully completed, as well as whether SEP has encountered an error	N/A
Pseudonymous general, statistical and status information	N/A

### How do I know that my Symantec Endpoint Protection clients are sending telemetry submissions?

Check the Client Activity log to view submissions events. If the log does not contain current submission events, check the following:

- Make sure that client submissions are enabled.
- If you use a proxy server, check the proxy exceptions. See [Can I specify a proxy server for client submissions?](#).
- Check connectivity to Symantec servers. See the knowledge base article, [https://support.symantec.com/en\\_US/article.TECH163042.html](https://support.symantec.com/en_US/article.TECH163042.html).
- Check to make sure that clients have current LiveUpdate content.  
Symantec Endpoint Protection uses a Submission Control Data (SCD) file. Symantec publishes the SCD file and includes it as part of a LiveUpdate package. Each Symantec product has its own SCD file. The SCD file controls the following settings:
  - How many submissions a client can submit in one day
  - How long to wait before the client software retries submissions
  - How many times to retry failed submissions
  - Which IP address of the Symantec Security Response server receives the submissions

If the SCD file becomes out-of-date, then the clients stop sending submissions. Symantec considers the SCD file out-of-date when client computers have not retrieved LiveUpdate content in 7 days. The client stops sending submissions after 14 days.

If clients stop the transmission of the submissions, the client software does not collect the submission information and send it later. When clients start to transmit submissions again, they only send the information about the events that occur after the transmission restart.

### Can I opt out of telemetry submission?

Yes, you can opt out. You can modify the server data collection or client submissions options in the client and the server user interfaces. However, Symantec recommends that you enable as much telemetry as possible to improve the security of your network.

## Performance, sizing, and deployment

### How much bandwidth does telemetry consume?

Symantec Endpoint Protection throttles client computer submissions to minimize any effect on your network. Symantec Endpoint Protection throttles submissions in the following ways:

- 
- Client computers only send samples when the computer is idle. Idle submission helps randomize the submissions traffic across the network.
  - Client computers send samples for unique files only. If Symantec has already seen the file, the client computer does not send the information.

#### **NOTE**

The data size of these submissions is very negligible. For instance, antivirus submissions do not typically exceed 4 KB and similarly IPS submissions are about 32 KB in size.

#### **Can I specify a proxy server for client submissions?**

You can configure the Symantec Endpoint Protection Manager to use a proxy server for submissions and other external communications that your Windows clients use. If your client computers use a proxy with authentication, you might need to specify exceptions for Symantec URLs in your proxy server configuration. The exceptions let your client computers communicate with Symantec Insight and other important Symantec sites.

For more details about the proxy, see:

[Specifying a proxy server for client submissions and other external communications](#)

To learn more about the exceptions for Symantec URLs, see:

[https://support.symantec.com/en\\_US/article.TECH162286.html](https://support.symantec.com/en_US/article.TECH162286.html)

## **Understanding server data collection and client submissions and their importance to the security of your network**

By default, Symantec Endpoint Protection clients and Symantec Endpoint Protection Manager submit some types of pseudonymous information to Symantec. Clients can also send non-pseudonymous data to Symantec to get customized analysis. You can control whether or not your clients or Symantec Endpoint Protection Manager submit information.

Both server data and client submissions are critical to improving the security of your network.

[What is server data collection?](#)

[What are pseudonymous client submissions?](#)

[What are non-pseudonymous client submissions? is this Windows only](#)

[Concerns about privacy](#)

[Concerns about bandwidth usage](#)

#### **What is server data collection?**

Server data is part of the information that helps Symantec measure and improve the efficacy of detection technologies.

#### **Symantec Endpoint Protection Manager submits the following types of pseudonymous information to Symantec:**

- Licensing information, which includes the name, version, language, and licensing entitlement data
- Usage of Symantec Endpoint Protection protection features
- Information about Symantec Endpoint Protection configuration. The information includes operating system information, server hardware and software configuration, CPU size, memory size, and software version and features for installed packages

You can change the server submissions setting during installation, or change the setting on the server's **Site Properties > Data Collection** tab in the console.

#### **NOTE**

Symantec always recommends that you keep server data collection enabled.

#### **What are pseudonymous client submissions?**

---

Symantec Endpoint Protection clients automatically submit pseudonymous information about detections, network, and configuration to Symantec Security Response. Symantec uses this pseudonymous information to address new and changing threats as well as to improve product performance. Pseudonymous data is not directly identified with a particular user.

The detection information that clients send includes information about antivirus detections, intrusion prevention, SONAR, and file reputation detections.

#### **NOTE**

Mac client submissions do not include SONAR or file reputation submissions. Linux clients do not support any client submissions.

#### **The pseudonymous information that clients send to Symantec benefits you by:**

- Increasing the security of your network
- Optimizing product performance

In some cases, however, you might want to prevent your clients from submitting some information. For example, your corporate policies might prevent your client computers from sending any network information to outside entities. You can disable a single type of submission, such as submission of network information, rather than disabling all types of client submissions.

#### **NOTE**

Symantec recommends that you always keep client submissions enabled. Disabling submissions might interfere with faster resolution of false positive detections on the applications that are used exclusively in your organization. Without information about the malware in your organization, product response and Symantec response to threats might take longer.

[Managing the pseudonymous or non-pseudonymous data that clients send to Symantec](#)

[How Symantec Endpoint Protection uses Symantec Insight to make decisions about files](#)

#### **What are non-pseudonymous client submissions?**

You can choose to submit non-pseudonymous client information to Symantec. This type of information provides insight into your security challenges that helps Symantec recommend customized solutions.

- You should use this option only if you participate in a Symantec-sponsored program that provides you custom analysis.
- The option is disabled by default.

[Managing the pseudonymous or non-pseudonymous data that clients send to Symantec](#)

#### **Concerns about privacy**

Symantec makes every attempt to pseudonymize the client submission data.

- Only suspicious executable files are submitted.
- User names are removed from path names.
- Computers and enterprises are identified by unique pseudonymized values.
- IP addresses are used for geographic location and then discarded.

For more information about privacy, see the following document:

[Privacy statement](#)

#### **Concerns about bandwidth usage**

Symantec Endpoint Protection minimizes the impact of client submissions on your network bandwidth.

You can check the Client Activity log to view the types of submissions that your client computers send and to monitor bandwidth usage.

## Managing the pseudonymous or non-pseudonymous data that clients send to Symantec

Symantec Endpoint Protection can protect computers by submitting pseudonymous information about detections to Symantec. Symantec uses this information to address new and changing threats. Any data you submit improves Symantec's ability to respond to threats and customize protection for your computers. Symantec recommends that you choose to submit as much detection information as possible.

### [Understanding server data collection and client submissions and their importance to the security of your network](#)

Client computers submit information pseudonymously about detections. You can specify the types of detections for which clients submit information. The data that Symantec telemetry collects may include pseudonymous elements that are not directly identifiable. Symantec neither needs nor seeks to use telemetry data to identify any individual user.

#### NOTE

Mac client submissions do not include SONAR or file reputation submissions. Linux clients do not support any client submissions.

To change client submission settings

1. In the console, select **Clients** then click the **Policies** tab.
2. In the **Settings** pane, click **External Communications Settings**.
3. Select the **Client Submissions** tab.
4. Enable or disable the **Send pseudonymous data to Symantec to receive enhanced threat protection intelligence** option.
5. Select **More options** if you want to enable or disable specific submission types, such as file reputation.
6. If you participate in a Symantec-sponsored custom analysis program, select **Send client-identifiable data to Symantec for custom analysis**.

#### WARNING

This option sends non-pseudonymous information to Symantec. Only use this option if you participate in a Symantec-sponsored program and want to share client-identifiable data with Symantec.

7. Select **OK**.

#### NOTE

On Mac clients, you can also disable IPS ping submissions. See the following article:

[How to disable IPS data submission on Symantec Endpoint Protection for Mac clients](#)

## How Symantec Endpoint Protection minimizes the impact of client submissions on your network bandwidth

Symantec Endpoint Protection throttles client computer submissions to minimize any effect on your network. Symantec Endpoint Protection throttles submissions in the following ways:

- 
- Client computers only send samples when the computer is idle. Idle submission helps randomize the submissions traffic across the network.
  - Client computers send samples for unique files only. If Symantec has already seen the file, the client computer does not send the information.
  - Symantec Endpoint Protection uses a Submission Control Data (SCD) file. Symantec publishes the SCD file and includes it as part of a LiveUpdate package. Each Symantec product has its own SCD file.

**The SCD file controls the following settings:**

- How many submissions a client can submit in one day
- How long to wait before the client software retries submissions
- How many times to retry failed submissions
- Which IP address of the Symantec Security Response server receives the submission

If the SCD file becomes out-of-date, then clients stop sending submissions. Symantec considers the SCD file out-of-date when a client computer has not retrieved LiveUpdate content in 7 days. The client stops sending submissions after 14 days.

If clients stop the transmission of the submissions, the client software does not collect the submission information and send it later. When clients start to transmit submissions again, they only send the information about the events that occur after the transmission restart.

[Understanding server data collection and client submissions and their importance to the security of your network](#)

## **Specifying a proxy server for client submissions and other external communications**

You can configure Symantec Endpoint Protection Manager to use a proxy server for submissions and other external communications that your Windows clients use.

### **NOTE**

If your client computers use a proxy with authentication, you might need to specify exceptions for Symantec URLs in your proxy server configuration. The exceptions let your client computers communicate with Symantec Insight and other important Symantec sites.

**You need to include exceptions for Symantec URLs in your proxy server settings if you use the following proxy configuration options:**

- You use a proxy server with authentication.
- You select **Use a proxy server specified by my client browser** option in the Symantec Endpoint Protection Manager **External Communication Dialog**.
- You use auto-detection or auto-configuration in your browser's Internet Options.

You do not have to specify exceptions for Symantec URLs in your proxy server settings if you do not use auto-detection or auto-configuration. You should select **Use custom proxy settings** in the **External Communication** dialog and then specify the authentication settings.

To specify a proxy server for client submissions and other external communications

1. In the console, on the **Clients** page, select the group and then click **Policies**.
2. Under **Settings** or **Location-specific Settings**, click **External Communications**.
3. On the **Proxy Server (Windows)** tab, under **HTTPS Proxy Configuration**, select **Use custom proxy settings**.
4. Enter the information about the proxy server that your clients use. See the online Help for more information about the options.
5. Click **OK**.

**For information about the recommended exceptions, see the following articles:**

- [How to test connectivity to Insight and Symantec licensing servers](#)
- [Required exclusions for proxy servers to allow Symantec Endpoint Protection to connect to Symantec reputation and licensing servers](#)

[Understanding server data collection and client submissions and their importance to the security of your network](#)

[Creating exceptions for Virus and Spyware scans](#)

## Managing SONAR

SONAR is part of Proactive Threat Protection on your client computers and the Virus and Spyware Protection policy in Symantec Endpoint Protection Manager.

**Table 118: Managing SONAR**

Task	Description
Learn how SONAR works	Learn how SONAR detects unknown threats. Information about how SONAR works can help you make decisions about using SONAR in your security network. <a href="#">About SONAR</a>
Check that SONAR is enabled	To provide the most complete protection for your client computers you should enable SONAR. SONAR interoperates with some other Symantec Endpoint Protection features. SONAR requires Auto-Protect. You can use the Clients tab to check whether Proactive Threat Protection is enabled on your client computers. <a href="#">Adjusting SONAR settings on your client computers</a>
Check the default settings for SONAR	SONAR settings are part of a Virus and Spyware Protection policy. <a href="#">About the default Virus and Spyware Protection policy scan settings</a>
Make sure that Insight lookups are enabled	SONAR uses reputation data in addition to heuristics to make detections. If you disable Insight lookups, SONAR makes detections by using heuristics only. The rate of false positives might increase, and the protection that SONAR provides is limited. You enable or disable Insight Lookups in the <b>Submissions</b> dialog. <a href="#">Understanding server data collection and client submissions and their importance to the security of your network</a>
Monitor SONAR events to check for false positive detections	You can use the SONAR log to monitor events. You can also view the SONAR Detection Results report (under Risk Reports) to view information about detections. <a href="#">Monitoring SONAR detection results to check for false positives</a> <a href="#">Monitoring endpoint protection</a>

Task	Description
Adjust SONAR settings	<p>You can change the detection action for some types of threats that SONAR detects. You might want to change the detection action to reduce false positive detections.</p> <p>You also might want to enable or disable notifications for high or low risk heuristic detections.</p> <p><a href="#">Adjusting SONAR settings on your client computers</a></p> <p><a href="#">Handling and preventing SONAR false positive detections</a></p>
Prevent SONAR from detecting the applications that you know are safe	<p>SONAR might detect the files or applications that you want to run on your client computers. You can use an Exceptions policy to specify exceptions for the specific files, folders, or applications that you want to allow. For the items that SONAR quarantines, you can create an exception for the quarantined item from the SONAR log.</p> <p>You also might want to set SONAR actions to log and allow detections. You can use application learning so that Symantec Endpoint Protection learns the legitimate applications on your client computers. After Symantec Endpoint Protection learns the applications that you use in your network, you can change the SONAR action to Quarantine.</p> <p><b>Note:</b> If you set the action for high risk detections to log only, you might allow potential threats on your client computers.</p> <p><a href="#">Handling and preventing SONAR false positive detections</a></p>
Prevent SONAR from examining some applications	<p>In some cases, an application might become unstable or cannot run when SONAR injects code into the application to examine it. You can create a file, folder, or application exception for the application.</p> <p><a href="#">Creating exceptions for Virus and Spyware scans</a></p>
Manage the way SONAR detects the applications that make DNS or host file changes	<p>You can use the SONAR policy settings to globally adjust the way SONAR handles detections of DNS or host file changes. You can use the Exceptions policy to configure exceptions for specific applications.</p> <p><a href="#">Adjusting SONAR settings on your client computers</a></p> <p><a href="#">Creating an exception for an application that makes a DNS or host file change</a></p>
Allow clients to submit information about SONAR detections to Symantec	<p>Symantec recommends that you enable submissions on your client computers. The information that clients submit about detections helps Symantec address threats. The information helps Symantec create better heuristics, which results in fewer false positive detections.</p> <p><a href="#">Understanding server data collection and client submissions and their importance to the security of your network</a></p>

## About SONAR

SONAR is a real-time protection that detects potentially malicious applications when they run on your computers. SONAR provides "zero-day" protection because it detects threats before traditional virus and spyware detection definitions have been created to address the threats.

SONAR uses heuristics as well as reputation data to detect emerging and unknown threats. SONAR provides an additional level of protection on your client computers and complements your existing Virus and Spyware Protection, intrusion prevention, Memory Exploit Mitigation, and firewall protection.

SONAR uses a heuristics system that leverages Symantec's online intelligence network with proactive local monitoring on your client computers to detect emerging threats. SONAR also detects changes or behavior on your client computers that you should monitor.

### NOTE

Auto-Protect also uses a type of heuristic that is called Bloodhound to detect suspicious behavior in files.

SONAR might inject some code into the applications that run in Windows user mode to monitor them for suspicious activity. In some cases, the injection might affect the application performance or cause problems with running the application. You can create an exception to exclude the file, folder, or application from this type of monitoring.

---

SONAR does not make detections on application type, but on how a process behaves. SONAR acts on an application only if that application behaves maliciously, regardless of its type. For example, if a Trojan horse or keylogger does not act maliciously, SONAR does not detect it.

SONAR detects the following items:

Heuristic threats	SONAR uses heuristics to determine if an unknown file behaves suspiciously and might be a high risk or low risk. It also uses reputation data to determine whether the threat is a high risk or low risk.
System changes	SONAR detects applications or the files that try to modify DNS settings or a host file on a client computer.
Trusted applications that exhibit bad behavior	Some good trusted files might be associated with suspicious behavior. SONAR detects these files as suspicious behavior events. For example, a well-known document sharing application might create executable files.

If you disable Auto-Protect, you limit SONAR's ability to make detections of high and low risk files. If you disable Insight lookups (reputation queries), you also limit the SONAR's detection capability.

[Managing SONAR](#)

[Managing exceptions in Symantec Endpoint Protection](#)

[Managing SONAR on your computer](#)

[Excluding items from scans](#)

## Handling and preventing SONAR false positive detections

SONAR might make false positive detections for certain internal custom applications. Also, if you disable Insight lookups, the number of false positives from SONAR increases.

[Understanding server data collection and client submissions and their importance to the security of your network](#)

You can change SONAR settings to mitigate false positive detections in general. You can also create exceptions for a specific file or a specific application that SONAR detects as a false positive.

### **WARNING**

If you set the action for high risk detections to log only, you might allow potential threats on your client computers.



**Table 119: Handling SONAR false positives**

Task	Description
Log SONAR high risk heuristic detections and use application learning	<p>You might want to set detection action for high risk heuristic detections to <b>Log</b> for a short period of time. Let application learning run for the same period of time. Symantec Endpoint Protection learns the legitimate processes that you run in your network. Some true detections might not be quarantined, however.</p> <p><a href="#">Collecting information about the applications that the client computers run</a></p> <p>After the period of time, you should set the detection action back to <b>Quarantine</b>.</p> <p><b>Note:</b> If you use aggressive mode for low risk heuristic detections, you increase the likelihood of false positive detections. Aggressive mode is disabled by default.</p> <p><a href="#">Adjusting SONAR settings on your client computers</a></p>
Create exceptions for SONAR to allow safe applications	<p><b>You can create exceptions for SONAR in the following ways:</b></p> <ul style="list-style-type: none"> <li>• Use the SONAR log to create an exception for an application that was detected and quarantined You can create an exception from the SONAR log for false positive detections. If the item is quarantined, Symantec Endpoint Protection restores the item after it rescans the item in the Quarantine. Items in the Quarantine are rescanned after the client receives updated definitions. <a href="#">Creating exceptions from log events</a></li> <li>• Use an Exceptions policy to specify an exception for a particular file name, folder name, or application. You can exclude an entire folder from SONAR detection. You might want to exclude the folders where your custom applications reside. <a href="#">Creating exceptions for Virus and Spyware scans</a></li> </ul>

## Adjusting SONAR settings on your client computers

You might want to change the SONAR actions to reduce the rate of false positive detections. You might also want to change the SONAR actions to change the number of detection notifications that appear on your client computers.

### NOTE

A cloud icon appears next to some options when this domain is enrolled in the cloud console. If an Intensive Protection policy is in effect, the policy overrides these options for 14.0.1 clients only.

To adjust SONAR settings on your client computers

1. In the Virus and Spyware Protection policy, select **SONAR**.
2. Make sure that **Enable SONAR** is checked.

### NOTE

When SONAR is enabled, Suspicious Behavior Detection automatically turns on. You cannot turn off Suspicious Behavior Detection when SONAR is enabled.

3. Under **Scan Details**, change the actions for high or low risk heuristic threats.

You can enable aggressive mode for low risk detections. This setting increases SONAR sensitivity to low risk detections. It might increase the false positive detections.

- 
- Optionally change the settings for the notifications that appear on your client computers.
  - Under **System Change Events**, change the action for either **DNS change detected** or **Host file change detected**.

#### NOTE

The **Prompt** action might result in many notifications on your client computers. Any action other than **Ignore** might result in many log events in the console and email notifications to administrators.

#### WARNING

If you set the action to **Block**, you might block important applications on your client computers.

For example, if you set the action to **Block** for **DNS change detected**, you might block VPN clients. If you set the action to **Block** for **Host file change detected**, you might block your applications that need to access the host file. You can use a DNS or host file change exception to allow a specific application to make DNS or host file changes.

[Creating an exception for an application that makes a DNS or host file change](#)

- Under **Suspicious Behavior Detection**, you can change the action for high or low risk detections.

If SONAR is disabled, you can also enable or disable Suspicious Behavior Detection.

- Click **OK**.

### Managing SONAR

#### [Creating exceptions for Virus and Spyware scans](#)

## Monitoring SONAR detection results to check for false positives

The client collects and uploads SONAR detection results to the management server. The results are saved in the SONAR log.

To determine which processes are legitimate and which are security risks, look at the following columns in the log:

Event	The event type and the action that the client has taken on the process, such as cleaning it or logging it. Look for the following event types: <ul style="list-style-type: none"><li>A possible legitimate process is listed as a <b>Potential risk found</b> event.</li><li>A probable security risk is listed as a <b>Security risk found</b> event.</li></ul>
Application	The process name.
Application type	The type of malware that a SONAR scan detected.
File/Path	The path name from where the process was launched.

The **Event** column tells you immediately whether a detected process is a security risk or a possible legitimate process. However, a potential risk that is found may or may not be a legitimate process, and a security risk that is found may or may not be a malicious process. Therefore, you need to look at the **Application type** and **File/Path** columns for more information. For example, you might recognize the application name of a legitimate application that a third-party company has developed.

To monitor SONAR detection results to check for false positives

- 
1. In the console, click **Monitors > Logs**.
  2. On the Logs tab, in the **Log type** drop-down list, click **SONAR**.
  3. Select a time from the **Time range** list box closest to when you last changed a scan setting.
  4. Click **Additional Settings**.
  5. In the **Event type** drop-down list, select one of the following log events:
    - To view all detected processes, make sure **All** is selected.
    - To view the processes that have been evaluated as security risks, click **Security risk found**.
    - To view the processes that have been evaluated and logged as potential risks, click **Potential risk found**.
  6. Click **View Log**.
  7. After you identify the legitimate applications and the security risks, create an exception for them in an Exceptions policy.

You can create the exception directly from the SONAR Logs pane.

#### [Creating exceptions from log events](#)

## Changing Tamper Protection settings

Tamper Protection provides real-time protection for Symantec applications that run on servers and clients. It prevents non-Symantec processes such as worms, Trojan horses, viruses, and security risks, from affecting Symantec resources. You can configure the client to block or log attempts to modify Symantec resources. You can create exceptions for the applications that Tamper Protection detects.

Tamper Protection settings are configured globally for a selected group.

To change Tamper Protection settings

1. In the console, click **Clients**.
2. On the **Policies** tab, under **Settings**, click **General Settings**.
3. On the **Tamper Protection** tab, check or uncheck **Protect Symantec security software from being tampered with or shut down**.
4. In the list box under **Actions to take if an application attempts to tamper with or shut down Symantec security software**, select one of the log actions.
5. Click **OK**.

#### [Creating a Tamper Protection exception on Windows clients](#)

## About application control, system lockdown, and device control

To monitor and control the behavior of applications on client computers, you use application control and system lockdown. Application control allows or blocks the defined applications that try to access system resources on a client computer. System lockdown allows only approved applications on client computers. To manage hardware devices that access client computers, you use device control.

### **WARNING**

Application control and system lockdown are advanced security features that only experienced administrators should configure.

You use application control, system lockdown, and device control for the following tasks.

Application control	<ul style="list-style-type: none"><li>• Prevent malware from taking over applications.</li><li>• Restrict the applications that can run.</li><li>• Prevent users from changing configuration files.</li><li>• Protect specific registry keys.</li><li>• Protect particular folders, such as \WINDOWS\system.</li></ul> <p>You configure application control and device control using an Application and Device Control policy.</p> <p><a href="#">Setting up application control</a></p>
System lockdown	<ul style="list-style-type: none"><li>• Control the applications on your client computers.</li><li>• Block almost any Trojan horse, spyware, or malware that tries to run or load itself into an existing application.</li></ul> <p>System lockdown ensures that your system stays in a known and trusted state.</p> <p><b>Note:</b> If you do not implement system lockdown carefully, it can cause serious problems in your network. Symantec recommends that you implement system lockdown in specific stages.</p> <p>You configure system lockdown in the <b>Policies</b> tab on the <b>Clients</b> page.</p> <p><a href="#">Configuring system lockdown</a></p>
Device control	<ul style="list-style-type: none"><li>• Block or allow different types of devices that attach to client computers, such as USB, infrared, and FireWire devices.</li><li>• Block or allow serial ports and parallel ports.</li></ul> <p><a href="#">Managing device control</a></p>

Both application control and device control are supported on 32-bit and 64-bit Windows computers.

As of 14, Mac computers support device control.

## Setting up application control

Application control allows or blocks the defined applications that try to access system resources on a client computer. You can allow or block access to certain registry keys, files, and folders. You can also define which applications are allowed to run, which applications that cannot be terminated through irregular processes, and which applications can call DLLs.

Use the following steps to set up application control on a group of client computers.

**Table 120: Setting up application control**

Steps	Description
Open a policy and enable default application control rule sets	<p>Application Control policies contain predefined rule sets, which are disabled by default. You can enable any sets that you need, and apply the policy to a group. The predefined rule sets are configured in production mode rather than test mode. However, you should change the setting to test mode and test the rules in your test network before you apply them to your production network.</p> <p><a href="#">Enabling and testing default application rules</a></p>
Add additional application control rules (optional)	<p>If the default rule sets do not meet your requirements, add new rule sets and rules. Typically, only advanced administrators should perform this task.</p> <p><a href="#">Adding custom rules to Application Control</a></p>
Add exceptions for applications	<p>Application control injects code in some applications to examine them, which can slow applications that run on the computer. If necessary, you can exclude some applications from application control. You use an Exceptions policy to add file exceptions or folder exceptions for application control.</p> <p><a href="#">Excluding a file or a folder from scans</a></p>

Steps	Description
View the Application Control logs	<p>If you are testing a new policy or are troubleshooting an issue, you should monitor application control events in the log.</p> <p>In both test mode and production mode, application control events are in the Application Control log in Symantec Endpoint Protection Manager. On the client computer, application control and device control events appear in the Control log.</p> <p>You might see duplicate or multiple log entries for a single application control action. For example, if explorer.exe tries to copy a file, it sets the write and delete bits of the file's access mask. Symantec Endpoint Protection logs the event. If the copy action fails because an application control rule blocks the action, explorer.exe tries to copy the file by using only the delete bit in the access mask. Symantec Endpoint Protection logs another event for the copy attempt.</p> <p><a href="#">Viewing logs</a></p>
Prevent or allow users from enabling or disabling application control (optional)	<p>In rare cases, application control might interfere with some safe applications that run on client computers. You might want to allow users to disable this option to troubleshoot problems. In the mixed mode or client mode, use the <b>Allow user to enable and disable the application device control</b> setting in the <b>Client User Interface Settings</b> dialog.</p> <p><a href="#">Preventing users from disabling protection on client computers</a></p>

You can also use system lockdown to allow approved applications or block unapproved applications on the client computers.

[Configuring system lockdown](#)

## Enabling and testing default application rules

Application control includes default rule sets that are made up of one or more rules. Default application control rule sets are installed with the Symantec Endpoint Protection Manager. The default rule sets are disabled at installation. To use the default rule sets in an Application Control policy, you must enable them and apply the policy to a group of clients.

For a description of the common predefined rules, see: [Hardening Symantec Endpoint Protection \(SEP\) with an Application and Device Control Policy to increase security](#)

In the following task you can enable and test the **Block writing to USB drives** rule set.

1. To enable a default application rule set, in the console, click **Policies > Application and Device Control**, and under **Tasks**, click **Add an Application Control Policy**.
2. In the **Overview** pane, type a name and description for the policy.
3. Click **Application Control**.
4. In the **Application Control** pane, check the **Enabled** check box next to each rule set that you want to implement.  
For example, next to the **Block writing to USB drives** rule set, check the check box in the Enabled column.
5. To review the rules for the rule set, select the rule, click **Edit**, and then click **OK**.

[Adding custom rules to Application Control](#)

6. Change **Production** to **Test (log only)**.
7. Assign the policy to a group, and click **OK**.
8. To test the rule set **Block writing to USB drives**, on the client computer, attach a USB drive.
9. Open Windows Explorer and double-click the USB drive.
10. Right-click the window and click **New > Folder**.

If application control is in effect, an **Unable to create folder** error message appears.

---

[About application control, system lockdown, and device control](#)

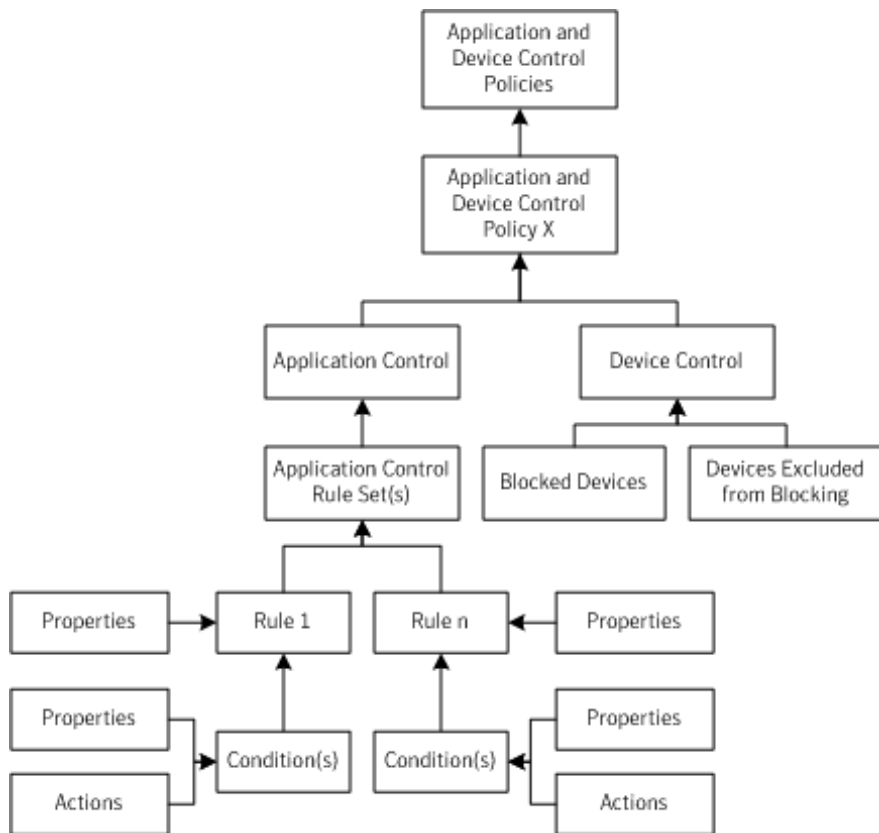
[About the structure of an Application Control and Device Control policy](#)

## The structure of an Application Control and Device Control policy

The Application and Device Control policy has two parts:

- Application Control contains one or more rule sets. Each rule set contains one or more rules. You configure properties, conditions, and actions for each rule:
  - **Rules** define the application(s) that you want to monitor.
  - **Conditions** monitor specified operations for the application(s) defined in the rule. The condition also contains the actions to take when the specified operation is observed.
  - As you add the rules and conditions, you need to specify the specific **properties** of the condition and what actions to take when the condition is met. Each condition type has different properties.
- Device control consists of a list of blocked devices and a list of devices that are excluded from blocking. You can add to these two lists and manage their contents.

[Application and Device Control policy structure](#) illustrates the application and device control components and how they relate to each other.



[About application control, system lockdown, and device control](#)

[Setting up application control](#)

[Adding custom rules to Application Control](#)

[Managing device control](#)

---

## Adding custom rules to Application Control

If the default rule sets do not meet your requirements, add new rule sets and rules. You can also modify the predefined rule sets that are installed with the policy.

- The rule set is the container that holds one or more rules that allows or blocks an action.
- The rules in the rule sets define one or more processes or applications. You can also exclude a process from being monitored.
- Each rule includes the conditions and the actions that apply to a given process or processes. For each condition, you can configure actions to take when the condition is met. You configure rules to apply to only certain applications, and you can optionally configure them to exclude other applications from having the action applied.

### [About the structure of an Application Control and Device Control policy](#)

Use the following steps to add your own application rules:

- [Step 1: Add a custom rule set and rules to an Application Control policy \(optional\)](#)
- [Step 2: Define the application or process for the rule \(optional\)](#)
- [Step 3: Add conditions and actions to a rule \(optional\)](#)
- Step 4: Test the rules before you apply them to your production network.

#### [Testing application control rules](#)

### Step 1: Add custom rule sets and rules

A best practice is to create a rule set that includes all of the actions that allow, block, and monitor a given task. On the other hand, you should create multiple rule sets if you have multiple tasks. For example, if you wanted to block write attempts to all removable drives and also block applications from tampering with a specific application, you should create two rules sets. You add and enable as many rule sets and rules as you need.

For example, BitTorrent is a communications protocol that is used for peer-to-peer file sharing and is not secure. BitTorrent distributes movies, games, music, and other files. BitTorrent is one of the simplest methods to distribute threats. Malware is hidden inside the files that are shared on peer-to-peer networks. You can use application control to block access to the BitTorrent protocol. You can also use peer-to-peer authentication and intrusion prevention. [Blocking a remote computer by configuring peer-to-peer authentication](#)

Consider the order of the rules and their conditions when you configure them to avoid unexpected consequences. Typically, only advanced administrators should perform this task.

### [Best practices for adding application control rules](#)

#### To add custom rule sets and rules

1. Open an Application Control policy.  
[Enabling and testing default application rules](#)
2. In the **Application Control** panel, under the list of default rule sets, click **Add**.  
To modify a predefined rule set, select it and then click **Edit**. For example, to monitor the applications that access the BitTorrent protocol, select **Block programs from running from removable drives [AC2]**.
3. In the **Add Application Control Rule Set** dialog box, type a name and description for the rule set.
4. Under Rules, select **Rule 1**, and on the **Properties** tab, type a meaningful name and description for the rule.  
To add an additional rule, click **Add > Add Rule**.

### Step 2: Define the application or process for the rule

Each rule must have at least one application or process that it monitors on the client computer. You can also exclude certain applications from the rule.

#### To define the application or process for the rule

1. With the rule selected, on the **Properties** tab, next to **Apply this rule to the following processes**, click **Add**.

2. In the **Add Process Definition** dialog box, type the application name or process name, such as `bittorrent.exe`.  
If you apply the rule to all applications except for a given set of applications, then define a wildcard for all (\*) in this step. Then list the applications that need to be exceptions next to **Do not apply this rule to the following processes**.
3. Click **OK**.

The **Enable this rule** check box is enabled by default. If you uncheck this option, the rule does not apply.

### Step 3: Add conditions and actions to a rule

The conditions control the behavior of the application or process that attempts to run on the client computer. Each condition type has its own properties to specify what the condition looks for.

Each condition has its own specific actions to take on the process when the condition is true. Except for the **Terminate** process action, the actions always apply to the process that you define for the rule, and not the condition.

**Warning:** The **Terminate** process action terminates the caller process, or the application that made the request. The caller process is the process that you define in the rule and not the condition. The other actions act on the target process, defined in the condition.

Condition	Description
<b>Registry Access Attempts</b>	Allows or blocks access to a client computer's registry settings.
<b>File and Folder Access Attempts</b>	Allows or blocks access to defined files or folders on a client computer.
<b>Launch Process Attempts</b>	Allows or blocks the ability to launch a process on a client computer.
<b>Terminate Process Attempts</b>	Allows or blocks the ability to terminate a process on a client computer. For example, you may want to block a particular application from being stopped. <b>Warning:</b> The <b>Terminate</b> Process Attempt condition refers to the target process. If you use the <b>Terminate Process Attempts</b> condition on Symantec Endpoint Protection or another important process and then use the <b>Terminate</b> process action to kill the process that tries to kill Symantec Endpoint Protection.
<b>Load DLL Attempts</b>	Allows or blocks the ability to load a DLL on a client computer.

1. Under **Rules**, select the rule you added, click **Add > Add Condition**, and choose a condition.  
[Best practices for choosing which condition to use for a rule](#)  
For example, click **Launch Process Attempts** to add a condition for when the client computer accesses the BitTorrent protocol.
2. On the **Properties** tab, select the process that should or should not be launched:
  - To specify a process to launch:  
Next to **Apply to the following entity**, click **Add**.
  - To exclude a process from being launched:  
Next to **Do not apply to the following processes**, click **Add**.
3. In the **Add entity Definition** dialog box, type process name, DLL, or registry key.  
For example, to add BitTorrent, type its file path and executable, such as: `C:\Users\UserName\AppData\Roaming\BitTorrent`  
To apply a condition to all processes in a particular folder, a best practice is to use `folder_name\*` or `folder_name\*\*`. One asterisk includes all the files and folders in the named folder. Use `folder_name\*\*` to include every file and folder in the named folder plus every file and folder in every subfolder.
4. Click **OK**.
5. On the **Actions** tab for the condition, select an action to take.  
For example, to block Textpad if it tries to launch Firefox, click **Block access**.
6. Check **Enable logging** and **Notify user**, and add a message you want the client computer user to see.  
For example, type `Textpad tries to launch Firefox`.



7. Click **OK**.

The new rule set appears and is configured for test mode. You should test new rule sets before you apply them to your client computers.

## Best practices for adding application control rules

You should plan your custom application control rules carefully. When you add application control rules, keep in mind the following best practices.

**Table 121: Best practices for application control rules**

Best practice	Description	Example
Consider the rule order	Application control rules work similarly to most network-based firewall rules in that both use the first rule match feature. When multiple conditions are true, the first rule is the only one that is applied unless the action that is configured for the rule is to <b>Continue processing other rules</b> .	You want to prevent all users from moving, copying, and creating files on USB drives. You have an existing rule with a condition that allows write access to a file named Test.doc. You add a second condition to this existing rule set to block all USB drives. In this scenario, users are still able to create and modify a Test.doc file on USB drives. The <b>Allow access</b> to Test.doc condition comes before the <b>Block access</b> to USB drives condition in the rule set. The <b>Block access</b> to USB drives condition does not get processed when the condition that precedes it in the list is true.
Use the right action	The <b>Terminate Process Attempts</b> condition allows or blocks an application's ability to terminate the calling process on a client computer. The condition does not allow or prevent users from stopping an application by the usual methods, such as clicking Quit from the File menu.	Process Explorer is a tool that displays the DLL processes that have opened or loaded, and what resources the processes use. You might want to terminate Process Explorer when it tries to terminate a particular application. Use the <b>Terminate Process Attempts</b> condition and the <b>Terminate process</b> action to create this type of rule. You apply the condition to the Process Explorer application. You apply the rule to the application or applications that you do not want Process Explorer to terminate.
Use one rule set per goal	Create one rule set that includes all of the actions that allow, block, or monitor a given task.	You want to block write attempts to all removable drives and you want to block applications from tampering with a particular application. To accomplish these goals, you should create two different rule sets instead of one rule set.
Use the <b>Terminate process</b> action sparingly	The <b>Terminate process</b> action kills the calling process when the process meets the configured condition. Only advanced administrators should use the <b>Terminate process</b> action. Typically, you should use the <b>Block access</b> action instead.	You want to terminate Winword.exe any time that any process launches Winword.exe. You create a rule and configure it with the <b>Launch Process Attempts</b> condition and the <b>Terminate process</b> action. You apply the condition to Winword.exe and apply the rule to all processes. You might expect this rule to terminate Winword.exe, but that is not what the rule does. If you try to start Winword.exe from Windows Explorer, a rule with this configuration terminates Explorer.exe, not Winword.exe. Users can still run Winword.exe if they launch it directly. Instead, use the <b>Block access</b> action, which blocks the target process, or Winword.exe.

Best practice	Description	Example
Test rules before you put them into production	The <b>Test (log only)</b> option for rule sets logs the actions, and does not apply to the actions to the client computer. Run rules in test mode for some acceptable period of time before you switch them back to production mode. During this time period, review the Application Control logs and verify that the rules work as planned.	The test option reduces potential accidents you might make by not considering all possibilities of the rule. <a href="#">Testing application control rules</a>

[Adding custom rules to Application Control](#)

[Best practices for choosing which condition to use for a rule](#)

## Best practices for choosing which condition to use for a rule

You add custom application control rules and conditions to prevent users from opening applications, writing to files, or sharing files. You can look at the default rule sets to help determine how to set up your rules. For example, you can edit the **Block applications from running** rule set to view how you might use a **Launch Process Attempts** condition.

[Adding custom rules to Application Control](#)

**Table 122: Typical conditions to use for a rule**

Rule	Condition
Prevent users from opening an application	<p><b>You can block an application when it meets either of these conditions:</b></p> <ul style="list-style-type: none"> <li>• <b>Launch Process Attempts</b> For example, to prevent users from transferring FTP files, you can add a rule that blocks a user from launching an FTP client from the command prompt.</li> <li>• <b>Load DLL Attempts</b> For example, if you add a rule that blocks Msvcr7.dll on the client computer, users cannot open Microsoft WordPad. The rule also blocks any other application that uses the DLL.</li> </ul>
Prevent users from writing to a particular file	<p>You may want to let users open a file but not modify the file. For example, a file may include the financial data that employees should view but not edit.</p> <p>You can create a rule to give users read-only access to a file. For example, you can add a rule that lets you open a text file in Notepad but does not let you edit it.</p> <p>Use the <b>File and Folder Access Attempts</b> condition for this type of rule.</p>
Block file shares on Windows computers	<p>You can disable local file and print sharing on Windows computers.</p> <p><b>Include the following conditions:</b></p> <ul style="list-style-type: none"> <li>• <b>Registry Access Attempts</b> Add all the relevant Windows security and sharing registry keys.</li> <li>• <b>Launch Process Attempts</b> Specify the server service process (svchost.exe).</li> <li>• <b>Load DLL Attempts</b> Specify the DLLs for the Security and Sharing tabs (rshx32.dll, ntshrui.dll).</li> <li>• <b>Load DLL Attempts</b> Specify the server service DLL (srvsvc.dll).</li> </ul> <p>You set the action for each condition to <b>Block access</b>.</p> <p>You can also use firewall rules to prevent or allow client computers to share files.</p> <p><a href="#">Permitting clients to browse for files and printers in the network</a></p>

Rule	Condition
Prevent users from running peer-to-peer applications	<p>You can prevent users from running peer-to-peer applications on their computers.</p> <p>You can create a custom rule with a <b>Launch Process Attempts</b> condition. In the condition, you must specify all peer-to-peer applications that you want to block, such as LimeWire.exe or *.torrent. You can set the action for the condition to <b>Block access</b>.</p> <p>Use an Intrusion Prevention policy to block network traffic from peer-to-peer applications. Use a Firewall policy to block the ports that send and receive peer-to-peer application traffic.</p> <p><a href="#">Managing intrusion prevention</a></p> <p><a href="#">Creating a firewall policy</a></p>
Block write attempts to DVD drives	<p>Currently, application control does not have a default rule that blocks CD/DVD writing directly. Instead, you create a rule that blocks the specific DLLs that write to CD or DVD drives using the <b>Add Condition</b> and <b>File and Folder Access Attempts</b> conditions.</p> <p>You should also create a Host Integrity policy that sets the Windows registry key to block write attempts to DVD drives.</p> <p><a href="#">Setting up Host Integrity</a></p> <p>See: <a href="#">How to block CD/DVD Writing in Windows 7</a></p>

## Testing application control rules

After you add application control rules, you should test them in your network. Configuration errors in the rule sets that are used in an Application Control policy can disable a computer or a server. The client computer can fail, or its communication with Symantec Endpoint Protection Manager can be blocked. After you test the rules, apply them to your production network.

### Step 1: Set the rule set to test mode

You test rule sets by setting the mode to test mode. Test mode creates a log entry to indicate when rules in the rule set would be applied without actually applying the rule.

Default rules use production mode by default. Custom rules use test mode by default. You should test both default and custom rules sets.

You might want to test rules within the set individually. You can test individual rules by enabling or disabling them in the rule set.

Changing a rule set to test mode

1. In the console, open an Application and Device Control policy.
2. Under **Application Control Policy**, click **Application Control**.
3. In the **Application Control Rule Sets** list, click the drop-down arrow in the **Test/Production** column for the rule set, and click **Test (log only)**.

[Setting up application control](#)

### Step 2: Apply the Application and Device Control policy to computers in your test network

If you created a new Application and Device Control policy, apply the policy to clients in your test network.

[Assigning a policy to a group or location](#)

### Step 3: Monitor the Application Control log

After you run your rule sets in test mode for a period of time, check the logs for any errors. In both test mode and production mode, application control events are in the Application Control log in Symantec Endpoint Protection Manager. On the client computer, application control and device control events appear in the Control log.

---

You might see duplicate or multiple log entries for a single application control action. For example, if explorer.exe tries to copy a file, it sets the write and delete bits of the file's access mask. Symantec Endpoint Protection logs the event. If the copy action fails because an application control rule blocks the action, explorer.exe tries to copy the file by using only the delete bit in the access mask. Symantec Endpoint Protection logs another event for the copy attempt.

[Viewing logs](#)

#### **Step 4: Change the rule set back to production mode**

When the rules function like you expect them to, change the rule set back to production mode.

## **Configuring system lockdown**

System lockdown controls applications on a group of client computers by blocking unapproved applications. You can set up system lockdown to allow only applications on a specified list. The allow list (whitelist) includes all the approved applications; any other applications are blocked on client computers. Or, you can set up system lockdown to block only applications on a specified list. The deny list (blacklist) comprises all the unapproved applications; any other applications are allowed on client computers.

### **NOTE**

Any applications that system lockdown allows are subject to other protection features in Symantec Endpoint Protection.

An allow list or deny list can include file fingerprint lists and specific application names. A file fingerprint list is a list of file checksums and computer path locations.

You can use an Application and Device Control policy to control specific applications instead of or in addition to system lockdown.

You set up system lockdown for each group or location in your network.

**Table 123: System lockdown steps**

Action	Description
Step 1: Create file fingerprint lists	<p>You can create a file fingerprint list that includes the applications that are allowed or not allowed to run on your client computers. You add the file fingerprint list to the allow list and deny list in system lockdown.</p> <p>When you run system lockdown, you need a file fingerprint list that includes the applications for all clients that you want to allow or block. For example, your network might include Windows 8.1 32-bit and 64-bit clients, and Windows 10 64-bit clients. You can create a file fingerprint list for each client image.</p> <p><b>You can create a file fingerprint list in the following ways:</b></p> <ul style="list-style-type: none"> <li>• Symantec Endpoint Protection provides a checksum utility to create a file fingerprint list. The utility is installed along with Symantec Endpoint Protection on the client computer. Use the utility to create a checksum for a particular application or all the applications in a specified path. Use this method to generate file fingerprints to use when you run system lockdown in deny mode. <a href="#">Creating a file fingerprint list with checksum.exe</a></li> <li>• Create a file fingerprint list on a single computer or small group of computers using the Collect File Fingerprint List command. You can run the <b>Collect File Fingerprint List</b> command from the console. The command collects a file fingerprint list that includes every application on the targeted computers. For example, you might run the command on a computer that runs a gold image. You can use this method when you run system lockdown in allow mode. Note that the file fingerprint list that you generate with the command cannot be modified. When you re-run the command, the file fingerprint list is automatically updated. <a href="#">Running commands on client computers from the console</a></li> <li>• Create a file fingerprint list with any third-party checksum utility.</li> </ul> <p><b>Note:</b> If you run Symantec EDR in your network, you might see file fingerprint lists from Symantec EDR.</p> <p><b>Note:</b> <a href="#">Interaction between system lockdown and Symantec EDR deny list (blacklist) rules</a></p>
Step 2: Import file fingerprint lists into Symantec Endpoint Protection Manager	<p>Before you can use a file fingerprint list in the system lockdown configuration, the list must be available in Symantec Endpoint Protection Manager.</p> <p>When you create file fingerprint lists with a checksum tool, you must manually import the lists into Symantec Endpoint Protection Manager. <a href="#">Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager</a></p> <p>When you create a file fingerprint list with the <b>Collect File Fingerprint List</b> command, the resulting list is automatically available in the Symantec Endpoint Protection Manager console.</p> <p>You can also export existing file fingerprint lists from Symantec Endpoint Protection Manager.</p>
Step 3: Create application name lists for approved or unapproved applications	<p>You can use any text editor to create a text file that includes the file names of the applications to allow or block. Unlike file fingerprint lists, you import these files directly into the system lockdown configuration. After you import the files, the applications appear as individual entries in the system lockdown configuration.</p> <p>You can also manually enter individual application names in the system lockdown configuration.</p> <p><b>Note:</b> A large number of named applications might affect client computer performance when system lockdown is enabled in deny mode.</p> <p><a href="#">Creating an application name list to import into the system lockdown configuration</a></p>

Action	Description
Step 4: Set up and test the system lockdown configuration	<p>In test mode, system lockdown is disabled and does not block any applications. All unapproved applications are logged but not blocked. You use the <b>Log Unapproved Applications Only</b> option in the <b>System Lockdown</b> dialog to test the entire system lockdown configuration.</p> <p><b>To set up and run the test, complete the following steps:</b></p> <ul style="list-style-type: none"> <li>• Add file fingerprint lists to the system lockdown configuration. In allow mode, the file fingerprints are approved applications. In deny mode, the file fingerprints are unapproved applications.</li> <li>• Add individual application names or import application name lists into the system lockdown configuration. You can import a list of application names rather than enter the names one by one in the system lockdown configuration. In allow mode, the applications are approved applications. In deny mode, the applications are unapproved applications.</li> <li>• Run the test for a period of time. Run system lockdown in test mode long enough so that clients run their usual applications. A typical time frame might be one week.</li> </ul> <p><a href="#">Setting up and testing the system lockdown configuration before you enable system lockdown</a></p>
Step 5: View the unapproved applications and modify the system lockdown configuration if necessary	<p>After you run the test for a period of time, you can check the list of unapproved applications. You can view the list of unapproved applications by checking the status in the <b>System Lockdown</b> dialog box.</p> <p>The logged events also appear in the Application Control log.</p> <p>You can decide whether to add more applications to the file fingerprint or the applications list. You can also add or remove file fingerprint lists or applications if necessary before you enable system lockdown.</p> <p><a href="#">Setting up and testing the system lockdown configuration before you enable system lockdown</a></p>
Step 6: Enable system lockdown	<p>By default, system lockdown runs in allow mode. You can configure system lockdown to run in deny mode instead.</p> <p>When you enable system lockdown in allow mode, you block any application that is not on the approved applications list. When you enable system lockdown in deny mode, you block any application that is on the unapproved applications list.</p> <p><b>Note:</b> Make sure that you test your configuration before you enable system lockdown. If you block a needed application, your client computers might be unable to restart.</p> <p><a href="#">Running system lockdown in allow mode</a>  <a href="#">Running system lockdown in deny mode</a></p>

Action	Description
Step 7: Update file fingerprint lists for system lockdown	<p>Over time, you might change the applications that run in your network. You can update your file fingerprint lists or remove lists as necessary.</p> <p><b>You can update file fingerprint lists in the following ways:</b></p> <ul style="list-style-type: none"> <li>Manually append, replace, or merge file fingerprint lists that you imported. You cannot append file fingerprint lists to a fingerprint list that you generate with the <b>Collect File Fingerprint List</b> command. You can append an imported list with a command-generated list. In that case, if you re-run the fingerprint command, you must recreate the appended list. <a href="#">Manually updating a file fingerprint list in Symantec Endpoint Protection Manager</a> <a href="#">Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager</a></li> <li>Automatically update existing file fingerprint lists that you imported. You can also automatically update applications or the application name lists that you import. <a href="#">Automatically update file fingerprint lists to allow or block for system lockdown</a> <a href="#">Creating an application name list to import into the system lockdown configuration</a></li> <li>Re-run the <b>Collect File Fingerprint List</b> command to automatically update a command-generated fingerprint list. When you re-run the command, the new list automatically replaces the existing list.</li> </ul> <p><b>Note:</b> You might want to re-test the entire system lockdown configuration if you add client computers to your network. You can move new clients to a separate group or test network and disable system lockdown. Or you can keep system lockdown enabled and run the configuration in log-only mode. You can also test individual file fingerprints or applications as described in the next step.</p>
Step 8: Test selected items before you add or remove them when system lockdown is enabled	<p>After system lockdown is enabled, you can test individual file fingerprints, application name lists, or specific applications before you add or remove them to the system lockdown configuration. You might want to remove file fingerprint lists if you have many lists and no longer use some of them.</p> <p><b>Note:</b> Be careful when you add or remove a file fingerprint list or a specific application from system lockdown. Adding or removing items from system lockdown can be risky. You might block important applications on your client computers.</p> <ul style="list-style-type: none"> <li>Test selected items. Use the <b>Test Before Removal</b> to log specific file fingerprint lists or specific applications as unapproved. When you run this test, system lockdown is enabled but does not block any selected applications or any applications in the selected file fingerprint lists. Instead, system lockdown logs the applications as unapproved.</li> <li>Check the Application Control log. The log entries appear in the Application Control log. If the log has no entries for the tested applications, then you know that your clients do not use those applications.</li> </ul>

## Setting up application control

### Creating a file fingerprint list with checksum.exe

You can use the checksum.exe utility to create a file fingerprint list. The list contains the following for each executable file or DLL that resides in a specified path on the computer:

- The path
- The file name
- The corresponding checksum

You then import the file fingerprint list into Symantec Endpoint Protection Manager to use in your system lockdown configuration.

---

The utility is installed with Symantec Endpoint Protection on the client computer.

### [Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager](#)

#### [Configuring system lockdown](#)

You can also use a third-party utility or the **Collect File Fingerprint List** command to create a file fingerprint list.

#### [Running commands on client computers from the console](#)

To create a file fingerprint list with checksum.exe

1. Open a command prompt window on the computer that contains the image for which you want to create a file fingerprint list.

The computer must have Symantec Endpoint Protection client software installed.

2. Navigate to the client installation folder, which contains the file checksum.exe. Typically, the file is located in the following folder:

C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\

3. Type the following command:

```
checksum.exe outputfile.txt path
```

Where:

- outputfile.txt is the name of the resulting text file that contains the checksums for all the applications that are located on the specified drive.
- path is the file path on the computer on which you want to gather checksum information.

#### **NOTE**

To run a checksum against all files on the C drive, you must add a forward slash at the end of path. Otherwise, the command only runs in the folder where `checksum.exe` is located.

The format of each line in the output file is as follows:

```
checksum_of_the_file full_pathname_of_the_exe_or_DLL
```

A space separates the checksum value and the full pathname.

An example of checksum.exe output is shown here:

```
0bb018fad1b244b6020a40d7c4eb58b7 c:\dell\openmanage\remind.exe
35162d98c2b445199fef95e838feae4b c:\dell\pnp\m\co\HSFCI008.dll
2f276c59243d3c051547888727d8cc78 c:\Nokia Video Manager\QtCore4.dll
```

#### **Example syntax**

The following is an example of the syntax you can use to create a fingerprint list for all of the files on the C drive:

```
checksum.exe cdrive.txt c:/
```

This command creates a file that is called cdrive.txt. It contains the checksums and file paths of all the executables and DLLs found on the C drive of the computer on which it runs.

#### **NOTE**

If the paths contain a space or if you use a batch file, enclose the paths with quotes (" "), such as: "C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\Checksum.exe" cdrive.txt c:/

The following is an example of the syntax that you can use to create a fingerprint for a folder on the client computer:

```
checksum.exe blocklist.txt c:\Files
```



---

This command creates a file that is called blocklist.txt. It contains the checksums and file paths of any executables and DLLs found in the Files folder.

#### NOTE

If the paths contain a space or if you use a batch file, enclose the paths with quotes (" "), such as: "C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\Checksum.exe" blocklist.txt "c:\Files with a space"

## Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager

File fingerprint lists must be available in the Symantec Endpoint Protection Manager console so that you can add them to the system lockdown configuration. When you create file fingerprint lists with the checksum.exe utility or a third-party checksum tool, you must manually import the lists. You can also merge file fingerprint lists.

File fingerprint lists that you create with the Collect File Fingerprint List command are automatically available in the console. You do not need to import them. You cannot modify file fingerprint lists that you created with the Collect File Fingerprint List command. You can, however, merge a command-generated file fingerprint list with another file fingerprint list. If you run the command again to re-generate the list, you must manually merge the lists again.

### Configuring system lockdown

#### Creating a file fingerprint list with checksum.exe

Importing or merging file fingerprint lists

1. In the console, click **Policies**.
2. Under **Policies**, expand **Policy Components**, and then click **File Fingerprint Lists**.
3. Under **Tasks**, click **Add a File Fingerprint List**.
4. In the **Welcome to the Add File Fingerprint Wizard**, click **Next**.
5. In the **Information about New File Fingerprint** panel, type a name and description for the new list.
6. Click **Next**.
7. In the **Create a File Fingerprint** panel, select one of the following options:
  - **Create the file fingerprint by importing a file fingerprint file**
  - **Create the file fingerprint by combining multiple existing file fingerprints**  
This option is only available if you have already imported multiple file fingerprint lists.
8. Click **Next**.
9. Do one of the following actions:
  - Specify the path to the file fingerprint that you created. You can browse to find the file.
  - Select the fingerprint lists that you want to merge.
10. Click **Next**.
11. Click **Close**.
12. Click **Finish**.

The imported or merged fingerprint list appears under on the **Policies** tab under **Policies > Policy Components > File Fingerprint Lists**.

---

## Manually updating a file fingerprint list in Symantec Endpoint Protection Manager

You might want to update your file fingerprint lists after you run system lockdown for a while. You can append, replace, or remove entries in an existing file fingerprint list that you imported. You cannot directly edit any existing file fingerprint list in Symantec Endpoint Protection Manager.

If you want to merge fingerprint lists into a new list with a different name, use the **Add a File Fingerprint Wizard**.

If you create a fingerprint list with the Collect File Fingerprint List command, you cannot append, replace, or remove the entries. You can, however, append a command-generated list to an imported list. If you re-run the command, you must manually update the fingerprint list again.

You cannot modify any file fingerprint list that Symantec EDR sends to Symantec Endpoint Protection Manager.

[Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager](#)

[Configuring system lockdown](#)

To update a file fingerprint list in Symantec Endpoint Protection Manager

1. In the console, click **Policies**.
2. Under **Policies**, expand **Policy Components**, and then click **File Fingerprint Lists**.
3. In the **File Fingerprint Lists** pane, select the fingerprint list that you want to edit.
4. Click **Edit**.
5. In the **Edit File Fingerprint Wizard**, click **Next**.
6. Do one of the following:
  - Click **Append a fingerprint file to this file fingerprint** to add a new file to an existing one.
  - Click **Append another file fingerprint to this file fingerprint** to merge file fingerprint lists that you already imported.
  - Click **Replace an existing list with a new one**.
  - Click **Remove any fingerprints that also appear on a new list**.
7. Do one of the following:
  - Click **Browse** to locate the file or type the full path of the file fingerprint list that you want to append, replace, or remove.
  - Select the file fingerprints that you want to merge.
8. Click **Next > Close > Finish**.

## Interaction between system lockdown and Symantec EDR deny list (blacklist) rules

If your network includes Symantec EDR, you might see blocked applications in the system lockdown configuration from Symantec EDR.

Symantec EDR deny lists (blacklists) interact with the system lockdown configuration in the following ways:

- 
- When Symantec Endpoint Protection Manager receives a deny list rule from Symantec EDR, Symantec Endpoint Protection Manager enables system lockdown in deny mode for all domains and groups.
  - The deny list rule appears in the Symantec Endpoint Protection Manager file fingerprint list in the system lockdown configuration. You cannot modify a file fingerprint list from Symantec EDR.
  - If you configured a client group with system lockdown enabled in allow mode, the setting is preserved and Symantec Endpoint Protection Manager does not use the Symantec EDR deny list rule.
  - If you disable system lockdown and delete the Symantec EDR deny list, Symantec Endpoint Protection Manager automatically re-enables system lockdown and applies the deny list.
  - If you disable system lockdown but do not delete the Symantec EDR deny list, system lockdown remains disabled until you re-enable it.

#### NOTE

Symantec EDR sends allow list rules directly to Symantec Endpoint Protection clients. Symantec EDR does not send allow list file fingerprints to Symantec Endpoint Protection Manager.

[Running system lockdown in allow mode](#)

[Running system lockdown in deny mode](#)

[Configuring client groups to use private servers for reputation queries and submissions](#)

## Creating an application name list to import into the system lockdown configuration

You can import a list of application names into the system lockdown configuration. You might want to import an application name list rather than adding application names individually to the system lockdown configuration.

By default, 512 is the maximum number of applications that you can include in your combined application name lists. You can change the maximum in the `conf.properties` file.

You can create an application name list file with any text editor.

**Each line of the file can contain the following items each separated by a space:**

- The file name  
If you use a path name, it must be in quotes.
- The test mode  
The value should be 1 or Y for enabled or 0 or N for disabled. If you leave the field blank, test mode is disabled. You must include a value if you want to specify the matching mode.
- The matching mode (wildcard or regular expression)  
The value should be 1 or Y for regular expression matching or 0 or N for wildcard matching. If you leave the field blank, wildcard matching is used.

#### NOTE

The test mode field enables or disables the **Test Before Addition** or **Test Before Removal** option for each application in the list. The test mode field is ignored when you use the **Log Applications Only** option to test the entire system lockdown configuration.

Each line should use the following syntax:

```
filename test_mode matching_mode
```

For example:

```
aa.exe
bb.exe 0 1
cc.exe 1
dd.exe 1 0
```

```
"c:\program files\ee.exe" 0 0
```

When you import this list into system lockdown, the individual applications appear in the system lockdown configuration with the following settings:

**Table 124: Example matching mode settings**

Application Name	Test Before Addition or Test Before Removal	Matching Mode
aa.exe	Disabled	Wildcard
bb.exe	Disabled	Regular expression
cc.exe	Enabled	Wildcard
dd.exe	Enabled	Wildcard
c:\program files\ee.exe	Disabled	Wildcard

### [Configuring system lockdown](#)

## Automatically update file fingerprint lists to allow or block for system lockdown

Symantec Endpoint Protection Manager can automatically update existing file fingerprint lists and application name lists that you imported, merged, or appended.

File fingerprint lists that you generate from the **Collect File Fingerprint List** command are automatically updated when you re-run the command on the same computer.

You can also manually update existing file fingerprints.

**Table 125: Updating the allow list (whitelist) and deny list (blacklist) for system lockdown**

Step	Description
Step 1: Create updated file fingerprint lists or application name lists and compress the files	<p>You can use the checksum.exe utility or any third-party utility to create the updated file fingerprint lists. You can use any text editor to update application name lists. The lists must have the same names that already exist in Symantec Endpoint Protection Manager.</p> <p><a href="#">Creating a file fingerprint list with checksum.exe</a></p> <p>A fingerprint list that you generate from the <b>Collect File Fingerprint List</b> command cannot be updated directly. You can merge a command-generated list with another list, or append an imported list with a command-generated list.</p> <p>The automatic updates feature requires a compressed file (zip file) of the file fingerprint and application name lists. You can use the file compression feature in Windows or any compression utility to zip the files.</p>
Step 2: Create an index.ini file	<p>The index.ini file specifies which file fingerprint lists and application names lists Symantec Endpoint Protection Manager should update.</p> <p>You can create an index.ini file with any text editor and copy the file to the specified URL.</p> <p><a href="#">Creating an index.ini file for automatic updates of allow lists and deny lists that are used for system lockdown</a></p>

Step	Description
Step 3: Make the compressed file and index.ini available to Symantec Endpoint Protection Manager	<p>Symantec Endpoint Protection Manager uses UNC, FTP, or HTTP/HTTPS to retrieve the index.ini file and zip file at the specified URL. Symantec Endpoint Protection Manager uses the instructions in the index.ini file to update the specified files. When you enable automatic updates, Symantec Endpoint Protection Manager periodically checks the URL for updated files based on the schedule you set.</p> <p>For UNC, only JCFIS shares are supported. DFS shares are not supported.</p> <p><b>Note:</b> If you cannot use UNC, FTP, or HTTP/HTTPS, you can copy the index.ini and updated file fingerprint and application name files directly into the following folder: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\inbox\WhitelistBlacklist\content. The files should be unzipped. Symantec Endpoint Protection Manager checks this folder if it cannot use UNC, FTP, or HTTP/HTTPS to update the files.</p>
Step 4: Enable automatic allow list and deny list updates in the management console	<p>You must enable the automatic update of existing allow lists or deny lists in the Symantec Endpoint Protection Manager console.</p> <p>You use the <b>File Fingerprint Update</b> dialog in Symantec Endpoint Protection Manager to enable the update feature and specify the schedule and the URL information.</p> <p><a href="#">Enabling automatic updates of allow lists and deny lists for system lockdown</a></p>
Step 5: Check the status of automatic updates for the allow list or deny list	<p>You can make sure that Symantec Endpoint Protection Manager completes the updates by checking the status in the console.</p> <p>In the console, do one of the following actions:</p> <ul style="list-style-type: none"> <li>On the <b>Admin</b> tab, select the site. A message appears similar to the following message: <b>Update allow and deny lists for revision 20200528 R016 description succeeded.</b></li> <li>On the <b>Monitors</b> tab, view <b>System Logs: Server Activity</b>. The event type typically appears similar to <b>File fingerprint update</b>.</li> <li>On the <b>Policies</b> tab, under <b>Policy Components</b>, check the file fingerprint list description. The description appears similar to <b>Revision: 20200528 R016 description</b>.</li> </ul>

[Manually updating a file fingerprint list in Symantec Endpoint Protection Manager](#)

[Configuring system lockdown](#)

## Creating an index.ini file for automatic updates of allow lists and deny lists that are used for system lockdown

The automatic updates feature requires an index.ini file. You can create the file with any text editor.

### NOTE

If you use non-English characters in the text file, you should use UTF-8 without a byte order mark (BOM) character to edit and save the file.

### The index.ini file specifies the following items:

- The revision and name of the compressed file that includes your updated file fingerprint lists and application name lists.
- The names of the file fingerprint lists and application name lists that you want to update.
- The names of the client groups that use the application name lists.

The existing file fingerprint list or group must currently exist in Symantec Endpoint Protection Manager. The group must have system lockdown enabled. The file fingerprint lists and application name lists must be available in the specified compressed file.

You must structure the index.ini file with the following syntax:

```
[Revision]
```

---

```
Revision=YYYYMMDD RXXX
SourceFile=zip file name
Description=optional description
```

```
[FingerprintList - domain name or Default]
existing fingerprint list="updated list" REPLACE/APPEND/REMOVE
```

```
[ApplicationNameList - domain name or Default]existing group path="updated list" REPLACE/APPEND/REMOVE
```

For example, you could use the following lines in an index.ini file:

```
[Revision]
Revision=20111014 R001
SourceFile=20110901 R001.zip
Description=NewUpdates

[FingerprintList - Default]
FingerprintListName 1="FingerprintList1.txt" REPLACE
FingerprintListName 2="FingerprintList2.txt" REPLACE

[ApplicationNameList - Default]
My Company\Group AA\Group AA 1="ApplicationNameList1.txt" REPLACE
My Company\Group AA\Group AA 2="ApplicationNameList2.txt" REPLACE

[FingerprintList - DomainABC]
FingerprintListName 1="FingerprintList1.txt" REPLACE
FingerprintListName 2="FingerprintList2.txt" REPLACE

[ApplicationNameList - DomainABC]
My Company\Group AA\Group AA 1="ApplicationNameList1.txt" REPLACE
My Company\Group AA\Group AA 2="ApplicationNameList2.txt" REPLACE
```

[Automatically update file fingerprint lists to allow or block for system lockdown](#)

[Creating an application name list to import into the system lockdown configuration](#)

## Enabling automatic updates of allow lists and deny lists for system lockdown

You can configure Symantec Endpoint Protection Manager to automatically update allow lists (whitelists) and deny lists (blacklists) that you use for system lockdown.

To automatically update a file fingerprint list that you generated with the **Collect File Fingerprint List** command, first run the command.

1. In the console, on the **Admin** tab, click **Servers**.
2. Right-click the relevant server, and select **Edit the server properties**.
3. In the **Server Properties** dialog box, select the **File Fingerprint Update** tab.
4. On the **File Fingerprint Update** tab, check **Automatically update the allow or deny lists**.
5. Enter the URL for the location of the index.ini and the compressed file.

If you want to use UNC or FTP, you must also specify a user name and password for both the index.ini and the content.

- 
6. Under **Schedule**, you can specify how often Symantec Endpoint Protection Manager should try to update the list.
  7. Click **OK**.

[Automatically update file fingerprint lists to allow or block for system lockdown](#)

## Setting up and testing the system lockdown configuration before you enable system lockdown

Typically, you run system lockdown in test mode for a week, or enough time for clients to run their typical applications. After you determine that your system lockdown settings do not cause problems for users, you can enable system lockdown.

When you run system lockdown in test mode, system lockdown is disabled. System lockdown does not block any applications. Instead, unapproved applications are logged rather than blocked so that you can review the list before you enable system lockdown. You can view the log entries in the Control log. You can also view the unapproved applications in the **System Lockdown** dialog box.

### NOTE

You can also create firewall rules to allow approved applications on the client.

### To set up and test the system lockdown configuration before you enable system lockdown:

1. In the console, click **Clients**, then under **Clients**, locate the group for which you want to set up system lockdown.
2. On the **Policies** tab, click **System Lockdown**.
3. Click **Log Unapproved Applications Only** to run system lockdown in test mode.  
This option logs the unapproved applications that clients are currently running.
4. Select **Allow Mode** or **Deny Mode**.  
These options changed from **Whitelist Mode** or **Blacklist Mode** in 14.3 RU1.
5. Under **Application File Lists**, under **File Fingerprint List**, add or remove file fingerprint lists.  
To add a list, the list must be available in Symantec Endpoint Protection Manager.  
[Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager](#)
6. To add an application name list, under **Application File Lists**, under **File Name**, click **Import**.  
Specify the application name list that you want to import and click **Import**. The applications in the list appear as individual entries in the system lockdown configuration.  
The application name list must be a text file that specifies the file name, test mode, and matching mode.  
[Creating an application name list to import into the system lockdown configuration](#)
7. To add an individual application, under **Application File Lists**, under **File Name**, click **Add**.
8. In the **Add File Definition** dialog box, specify the full path name of the file (.exe or .dll).  
Names can be specified using a normal string or regular expression syntax. Names can include wildcard characters (\* for any characters and ? for one character). The name can also include environment variables such as %ProgramFiles% to represent the location of your Program Files directory or %windir% for the Windows installation directory.
9. Either leave **Use wildcard matching (\* and ? supported)** selected by default, or click **Use regular expression matching** if you used regular expressions in the file name instead.
10. If you want to allow the file only when it is executed on a particular drive type, click **Only match files on the following drive types**.  
Unselect the drive types you do not want to include. By default, all drive types are selected.
11. If you want to match by device ID type, check **Only match files on the following device id type**, and then click **Select**.
12. Click the device you want in the list, and then click **OK**.
13. Click **OK** to start the test.

After a period of time, you can view the list of unapproved applications. If you re-open the **System Lockdown for name of group** dialog box, you can see how long the test has been running.

---

### To view the unapproved applications that the test logged but did not block:

1. In the **System Lockdown name of group** dialog box, click **View Unapproved Applications**.
2. In the **Unapproved Applications** dialog box, review the applications.  
This list includes information about the time that the application was run, the computer host name, the client user name, and the executable file name.
3. Determine how you want to handle the unapproved applications.  
For allow mode, you can add the names of applications that you want to allow to the list of approved applications. For deny mode, you can remove the names of applications that you want to allow.
4. In the **Unapproved Applications** dialog, click **Reset the Test** if you changed the file fingerprint lists or individual applications and want to run the test again. Otherwise, click **Close**.
5. After you finish testing, you can enable system lockdown.

### [Configuring system lockdown](#)

## Running system lockdown in allow mode

You can configure system lockdown to allow only approved applications on your client computers. Only applications in the approved list are allowed to run. All other applications are blocked. The approved list is called an allow list (whitelist). Approved applications are subject to Symantec Endpoint Protection's other protection features.

### NOTE

By default, system lockdown runs in allow mode when you enable it.

### You should configure system lockdown to run in allow mode only after the following conditions are true:

- You tested the system lockdown configuration with the **Log Unapproved Applications Only** option.
- You are sure that all the applications that your client computers need to run are listed in the approved applications list.

### WARNING

Be careful when you add or remove a file fingerprint list or a specific application from system lockdown. Adding or removing items from system lockdown can be risky. You might block important applications on your client computers.

### [Setting up and testing the system lockdown configuration before you enable system lockdown](#)

### NOTE

If you run system lockdown enabled in allow mode, Symantec Endpoint Protection Manager does not apply any blocked applications from Symantec EDR.

### [Interaction between system lockdown and Symantec EDR deny list \(blacklist\) rules](#)

#### To run system lockdown in allow mode:

1. On the console, click **Clients**.
2. Under **Clients**, select the group for which you want to set up system lockdown.  
If you select a subgroup, the parent group must have inheritance turned off.



- 
3. On the **Policies** tab, click **System Lockdown**.
  4. Under **System Lockdown**, select **Enable System Lockdown** to block any unapproved applications that clients try to run.
  5. Under **Application File Lists**, select **Allow Mode (Whitelist Mode in 14.3 MP1 and earlier)**.
  6. Under **Approved Applications**, make sure that you have included all the applications that your client computers run.

#### **WARNING**

You must include all the applications that your client computers run in the approved applications list. If you do not, you could make some client computers unable to restart or prevent users from running important applications.

7. To display a message on the client computer when the client blocks an application, check **Notify the user if an application is blocked**.
8. Click **OK**.

[Configuring system lockdown](#)

[Disabling a group's inheritance](#)

## **Running system lockdown in deny mode**

You can enable system lockdown to block a list of unapproved applications on your client computers. All applications in the unapproved list are blocked. The unapproved list is called a deny list (blacklist). Any other applications are allowed. Allowed applications are subject to Symantec Endpoint Protection's other protection features.

#### **NOTE**

If you run Symantec EDR in your network, the Symantec EDR configuration affects the system lockdown allow list configuration.

[Interaction between system lockdown and Symantec EDR blacklist rules](#)

**You should configure system lockdown to block unapproved applications only after the following conditions are true:**

- You tested the system lockdown configuration with the **Log Unapproved Applications Only** option.
- You are sure that all of the applications that your client computers should block are listed in the unapproved applications list.

[Setting up and testing the system lockdown configuration before you enable system lockdown](#)

#### **WARNING**

Be careful when you add or remove a file fingerprint list or a specific application from system lockdown. Adding or removing items from system lockdown can be risky. You might block important applications on your client computers.

Running system lockdown in blacklist mode

1. On the console, click **Clients**.
2. Under **Clients**, select the group for which you want to set up system lockdown.  
If you select a subgroup, the parent group must have inheritance turned off.

[Disabling a group's inheritance](#)

3. On the **Policies** tab, select **System Lockdown**.
4. Under **System Lockdown** dialog box, select **Enable System Lockdown**.
5. Under **Application File Lists**, select **Deny Mode**. This option is **Blacklist Mode** in 14.3 MP1 and earlier.
6. Under **Unapproved Applications**, make sure that you have included all the applications that your client computers should block.

#### NOTE

A large number of named applications might decrease your client computer performance.

7. To display a message on the client computer when the client blocks an application, check **Notify the user if an application is blocked**.
8. Click **OK**.

[Setting up and testing the system lockdown configuration before you enable system lockdown](#)

[Configuring system lockdown](#)

## Managing device control

Device control specifies what hardware devices are allowed or blocked on your client computers. You use the default hardware devices list and a Device Control policy to manage device control. You can also add your own.

**Table 126: Managing device control**

Step	Description
Review the default hardware devices list in Symantec Endpoint Protection Manager	By default, Symantec Endpoint Protection Manager includes a list of hardware devices. The list appears on the <b>Policies</b> tab in Symantec Endpoint Protection Manager under <b>Policy Components</b> . You use this list to select the devices that you want to control on your client computers. If you want to control a device that is not included in the list, you must add the device first. <a href="#">About the hardware devices list</a>
Add devices to the hardware device list (if necessary)	When you add a device to the device list, you need a class ID or device ID for the device. You cannot add a customized device for Mac. You can only use the device types that are provided. <a href="#">Adding a hardware device to the Hardware Devices list</a> <a href="#">Obtaining a device vendor or model for Windows computers with DevViewer</a>
Allow or block a device in the Device Control policy	Specify the devices that you want to allow or block from being accessed on the client. <a href="#">Allowing or blocking devices on client computers</a>

For Mac clients, device control is part of SymDaemon service. You do not need to restart the Windows client or the Mac client for device control to work.

[About application control, system lockdown, and device control](#)

## Allowing or blocking devices on client computers

You use an Application and Device Control policy to configure device control. Before you begin, add any devices you need to the **Hardware Devices** list.

[Adding a hardware device to the Hardware Devices list](#)

---

As of 14, you can configure both Windows and Mac device control.

1. **Option 1:** To configure device control for Windows clients, in the console, open an Application and Device Control policy.
2. Click **Device Control**.
3. Under **Blocked Devices**, click **Add**.
4. In the **Device Selection** window, select one or more devices. Make sure that if you block specific ports, then you exclude devices if necessary.

**NOTE**

Typically, you should never block a keyboard.

5. Click **OK**.
6. Under **Devices Excluded From Blocking**, click **Add**.
7. In the **Device Selection** window, select one or more devices.
8. Check **Notify users when devices are blocked** if you want to notify the user.
9. Click **OK**.
10. **Option 2:** To configure device control for Mac clients (as of 14), in the console, open an Application and Device Control policy.
11. Under **Mac Settings**, click **Device Control**.
12. Under **Blocked Devices**, click **Add**.
13. In the **Device Selection** window, select a device from the list. You can only add one device at a time.

Fill in the fields at the bottom of the window, if available. If you leave the fields blank, all devices of this type are blocked.

You can also use regular expressions to define device vendor, device model, or serial number. See the Help in the **Mac Device Control** window for more information.

To obtain the serial number, model number, or vendor name from a Mac-connected device, use the DeviceInfo tool from the installation file. You can find this tool and its instructions under `Tools/DeviceInfo`.

14. Click **OK**.
15. Under **Devices Excluded From Blocking**, click **Add**.
16. In the **Device Selection** window, select a device from the list, define the excluded devices, and then click **OK**.
17. Check **Notify users when devices are blocked** if you want to notify the user.
18. Click **OK**.

[Mac Device Control](#)

[Managing device control](#)

[About application control, system lockdown, and device control](#)

## About the hardware devices list

Symantec Endpoint Protection Manager includes a hardware devices list. Some devices are included in the list by default. You use the devices when you configure device control.

[Managing device control](#)

---

You can add devices to the list. You cannot edit or delete any default devices.

You cannot add a customized hardware device for Mac.

Devices are identified by a device ID or class ID. You use either of these values to add a device to the list. You can use a tool to determine the device ID or the class ID. For Windows, go to Tools\DevViewer. For the Mac, go to Tools\DeviceInfo.

#### Obtaining a device vendor or model for Windows computers with DevViewer

class ID	The class ID refers to the Windows GUID. Each device type has both a Class and a ClassGuid associated with it. The ClassGuid is a hexadecimal value with the following format: {00000000-0000-0000-0000-000000000000}
device ID	A device ID is the most specific ID for a device. The syntax of a device ID includes some descriptive strings that make it easier to read than the class ID. When you add a device ID, you can use a device's specific ID. Alternately, you can use a wildcard character in the device ID string to indicate a less specific group of devices. You can use an asterisk (*) to indicate zero or more additional characters or a question mark (?) to indicate a single character of any value. The following is a device ID for a specific USB SanDisk device: USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_MICRO&REV_2033\0002071406&0 The following is a device ID with a wildcard that indicates any USB SanDisk device: USBSTOR\DISK&VEN_SANDISK* The following is a device ID with a wildcard that indicates any USB disk device: USBSTOR\DISK* The following is a device ID with a wildcard that indicates any USB storage device: USBSTOR*

#### Obtaining a device vendor or model for Windows computers with DevViewer

You can use the Symantec DevViewer tool to obtain either the class ID (GUID) or the device ID. You can use Windows Device Manager to obtain the device ID.

After you obtain a device ID, you can modify it with a wildcard character to indicate a less specific group of devices.

1. Download DevViewer to the client computer from the Attachments section at: [Use DevViewer to find hardware device IDs for Device Blocking in Endpoint Protection](#)
2. On the client computer, run `DevViewer.exe`.
3. Expand the Device Tree and locate the device for which you want the device ID or the GUID.  
For example, expand **Disk drives** and select the device within that category.
4. In the right-hand pane, right-click the device ID (which begins with [device ID]), and then click **Copy Device ID**.
5. Click **Exit**.
6. On the management server, paste the device ID into the list of hardware devices.
7. To obtain a device ID from Control Panel, open the Device Manager from the Control Panel.

The path to the Device Manager depends on the Windows operating system. For example, in Windows 7, click **Start > Control Panel > System > Device Manager**.

8. In the **Device Manager** dialog box, right-click the device, and click **Properties**.
9. In the device's **Properties** dialog box, on the **Details** tab, select the Device ID.

By default, the Device ID is the first value displayed.

---

10. Copy the ID string.

11. Click **OK**.

[Adding a hardware device to the Hardware Devices list](#)

[About class IDs](#)

[About device IDs](#)

## About class IDs

The class ID refers to the Windows GUID. Each device type has both a Class and a ClassGuid associated with it. The ClassGuid is a hexadecimal value with the following format:

```
{00000000-0000-0000-0000-000000000000}
```

[Obtaining a device vendor or model for Windows computers with DevViewer](#)

## About device IDs

A device ID is the most specific ID for a device. The syntax of a device ID includes some descriptive strings that make it easier to read than the class ID.

When you add a device ID, you can use a device's specific ID. Alternately, you can use a wildcard character in the device ID string to indicate a less specific group of devices. You can use an asterisk (\*) to indicate zero or more additional characters or a question mark (?) to indicate a single character of any value.

The following is a device ID for a specific USB SanDisk device:

```
USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_MICRO&REV_2033\0002071406&0
```

The following is a device ID with a wildcard that indicates any USB SanDisk device:

```
USBSTOR\DISK&VEN_SANDISK*
```

The following is a device ID with a wildcard that indicates any USB disk device:

```
USBSTOR\DISK*
```

The following is a device ID with a wildcard that indicates any USB storage device:

```
USBSTOR*
```

[Obtaining a device vendor or model for Windows computers with DevViewer](#)

## Adding a hardware device to the Hardware Devices list

After you obtain a class ID or device ID for a hardware device, you can add the hardware device to the default Hardware Devices list. You can then access this default list from the device control part of the Application and Device Control policy.

[About the hardware devices list](#)

To add hardware devices to the Hardware Devices list

1. In the console, click **Policies**.
  2. Under **Policies**, expand **Policy Components** and click **Hardware Devices**.
  3. Under **Tasks**, click **Add a Hardware Device**.
  4. Enter the name of the device you want to add.  
Both Class IDs and Device IDs are enclosed in curly braces ( { } ) by convention. You may need to replace the curly braces with the wildcard character ?.
  5. Select either **Class ID** or **Device ID**, and paste the ID that you copied from the Windows Device Manager or the DevViewer tool.
  6. You can use wildcard characters to define a set of device IDs. For example, you can use the following string: \*IDE \DVDROM\*.
- [Obtaining a device vendor or model for Windows computers with DevViewer](#)
7. Click **OK**.

## Managing exceptions in Symantec Endpoint Protection

You can manage exceptions for Symantec Endpoint Protection in the Symantec Endpoint Protection Manager console.

**Table 127: Managing exceptions**

Task	Description
Learn about exceptions	You use exceptions to exclude items from being scanned on your client computers.
Review the types of files and folders that Symantec Endpoint Protection automatically excludes from scans	Symantec Endpoint Protection automatically creates exceptions, or exclusions, for some third-party applications and some Symantec products. You can also configure individual scans to scan only certain extensions and skip any other extensions. <a href="#">About the files and folders that Symantec Endpoint Protection excludes from virus and spyware scans</a>
Create exceptions for scans	You add exceptions in an Exceptions policy directly. Or you can add exceptions from log events on the <b>Monitors</b> page. <a href="#">Creating exceptions for Virus and Spyware scans</a> <a href="#">Creating exceptions from log events</a>
Restricting the types of exceptions that users can configure on client computers (Windows only)	By default, users on client computers have limited configuration rights for exceptions. You can restrict users further so that they cannot create exceptions for virus and spyware scans or for SONAR. Users can never force an application detection and they never have permission to create Tamper Protection exceptions. Users also cannot create a file exception for application control. <a href="#">Restricting the types of exceptions that users can configure on client computers</a>
Check the logs for detections for which you might want to create exceptions	After Symantec Endpoint Protection makes a detection, you can create an exception for the detection from the log event. For example, you might want to create an exception for a file that scans detect but that your users request to download. <a href="#">Creating exceptions from log events</a>
Create exceptions for intrusion prevention signatures	You can specify exceptions for intrusion prevention. You can also set up a list of excluded hosts for intrusion prevention. Intrusion prevention exceptions are configured in an Intrusion Prevention policy. <a href="#">Creating exceptions for IPS signatures</a>

## Which Windows exceptions do I use for what type of scan?

[Exception names](#) lists which exception types are used in the Exceptions policy for which types of scans in Version 14 MPx and earlier.

**Table 128: Exception names**

Symantec Endpoint Protection Manager	Client restrictions (on Symantec Endpoint Protection Manager)*	Windows client	What is exception used for?
Application	Application Exception	Application Exception	<ul style="list-style-type: none"> <li>Auto-Protect</li> <li>Manual scans</li> <li>Scheduled scans</li> <li>Download Insight</li> <li>SONAR</li> </ul>
Application to Monitor	Not available	Not available	Application Control
Certificate	Not available	Not available	<ul style="list-style-type: none"> <li>Auto-Protect</li> <li>Manual scans</li> <li>Scheduled scans</li> <li>Download Insight</li> <li>SONAR</li> </ul>
DNS or Host File Change	DNS or Host File Change Exception	DNS or Host File Change Exception > Application	SONAR
Extensions	Extensions Exception	Security Risk Exception > Extensions	<ul style="list-style-type: none"> <li>Auto-Protect</li> <li>Manual scans</li> <li>Scheduled scans</li> </ul>
File	File Exception	Security Risk Exception > File	<ul style="list-style-type: none"> <li>Auto-Protect</li> <li>Manual scans</li> <li>Scheduled scans</li> <li>SONAR</li> <li>Application Control</li> </ul>
File Access	File Access		Application Control
Folder	Folder Exception: <ul style="list-style-type: none"> <li>Security risk Exception</li> <li>SONAR Exception</li> </ul>	Security Risk Exception > Folder SONAR Exception	<ul style="list-style-type: none"> <li>Auto-Protect</li> <li>Manual scans</li> <li>Scheduled scans</li> <li>SONAR</li> <li>Application Control</li> </ul>
Known Risks	Known risks Exception	Security Risk Exception > Known Risks	<ul style="list-style-type: none"> <li>Auto-Protect</li> <li>Manual scans</li> <li>Scheduled scans</li> <li>SONAR</li> </ul>
Trusted Web Domain	Trusted web domain Exception	Security Risk Exception > Web Domain	Download Insight
Tamper Protection Exception	Not available	Not available	Applications that Tamper Protection protects

\*Client restrictions are the exceptions that you can display or hide on the client for the client user to add. Exceptions that you add in the cloud console are unavailable in Symantec Endpoint Protection Manager to enable or disable on the client.

[Restricting the types of exceptions that users can configure on client computers](#)

## Creating exceptions for Virus and Spyware scans

You can create different types of exceptions for Symantec Endpoint Protection.

Any exception that you create takes precedence over any exception that a user might define. On client computers, users cannot view the exceptions that you create. A user can view only the exceptions that the user creates.

Exceptions for virus and spyware scans also apply to Download Insight.

**Table 129: Creating exceptions for Symantec Endpoint Protection**

Task	Description
Exclude a file from virus and spyware scans	Supported on Windows and Mac clients. Excludes a file by name from virus and spyware scans, SONAR, or application control on Windows clients. <a href="#">Excluding a file or a folder from scans</a>
Exclude a folder from virus and spyware scans	Supported on Windows, Mac, and Linux clients. Excludes a folder from virus and spyware scans, SONAR, or all scans on Windows clients. On Windows and Linux clients, you can choose to limit an exception for virus and spyware scans to Auto-Protect or scheduled and on-demand scans only. If you run an application that writes many temp files to a folder, you might want to exclude the folder from Auto-Protect. Auto-Protect scans files as they are written so you can increase computer performance by limiting the exception to scheduled and on-demand scans. You might want to exclude the folders that are not often used or that contain archived or packed files from scheduled and on-demand scans. For example, scheduled or on-demand scans of deeply archived files that are not often used might decrease computer performance. Auto-Protect still protects the folder by scanning only when any files are accessed or written to the folder. <a href="#">Excluding a file or a folder from scans</a>
Exclude a known risk from virus and spyware scans	Supported on Windows clients. Excludes a known risk from virus and spyware scans. The scans ignore the risk, but you can configure the exception so that the scans log the detection. In either case, the client software does not notify users when it detects the specified risks. If a user configures custom actions for a known risk that you configure to ignore, Symantec Endpoint Protection ignores the custom actions. Security risk exceptions do not apply to SONAR. <a href="#">Excluding known risks from virus and spyware scans on Windows clients</a>
Exclude file extensions from virus and spyware scans	Supported on Windows and Linux clients. Excludes any files with the specified extensions from virus and spyware scans. Extension exceptions do not apply to SONAR or to Power Eraser. <a href="#">Excluding file extensions from virus and spyware scans on Windows clients and Linux clients</a>
Monitor an application to create an exception for the application	Supported on Windows clients. Use the <b>Application to monitor</b> exception to monitor a particular application. When Symantec Endpoint Protection learns the application, you can create an exception to specify how Symantec Endpoint Protection handles the application. If you disable application learning, the Application to monitor exception forces application learning for the application that you specify. <a href="#">Monitoring an application to create an exception for the application on Windows clients</a>



Task	Description
Specify how virus and spyware scans handle monitored applications	<p>Supported on Windows clients.</p> <p>Use an application exception to specify an action for Symantec Endpoint Protection to apply to a monitored application. The type of action determines whether Symantec Endpoint Protection applies the action when it detects the application or when the application runs. Symantec Endpoint Protection applies the Terminate, Quarantine, or Remove action to an application when it launches or runs. It applies the Log only or Ignore action when it detects the application.</p> <p>Unlike a file name exception, an application exception is a hash-based exception. Different files can have the same name, but a file hash uniquely identifies an application.</p> <p>The application exception is a SHA-2 hash-based exception.</p> <p>Applications for which you can create exceptions appear in the <b>Exceptions</b> dialog after Symantec Endpoint Protection learns the application. You can request that Symantec Endpoint Protection monitors a specific application to learn.</p> <p><a href="#">Specifying how Symantec Endpoint Protection handles monitored applications on Windows clients</a>  <a href="#">Collecting information about the applications that the client computers run</a></p>
Exclude a web domain from virus and spyware scans	<p>Supported on Windows clients.</p> <p>Download Insight scans the files that users try to download from websites and other portals. Download Insight runs as part of a virus and spyware scan. You can configure an exception for a specific web domain that you know is safe.</p> <p>Download Insight must be enabled for the exception to have any effect.</p> <p><b>Note:</b> If your client computers use a proxy with authentication, you must specify trusted web domain exceptions for Symantec URLs. The exceptions let your client computers communicate with Symantec Insight and other important Symantec sites.</p> <p><b>See the following articles:</b></p> <ul style="list-style-type: none"> <li>• <a href="#">How to test connectivity to Insight and Symantec licensing servers</a></li> <li>• <a href="#">Required exclusions for proxy servers to allow Symantec Endpoint Protection to connect to Symantec reputation and licensing servers</a></li> </ul> <p><a href="#">Excluding a trusted web domain from scans on Windows clients</a></p>
Create file exceptions for Tamper Protection	<p>Supported on Windows clients.</p> <p>Tamper Protection protects client computers from the processes that tamper with Symantec processes and internal objects. When Tamper Protection detects a process that might modify the Symantec configuration settings or Windows registry values, it blocks the process.</p> <p>Some third-party applications inadvertently try to modify Symantec processes or settings. You might need to allow a safe application to modify Symantec settings. You might want to stop Tamper Protection for certain areas of the registry or certain files on the client computer.</p> <p>In some cases, Tamper Protection might block a screen reader or some other assistive technology application. You can create a file exception so that the application can run on client computers. Folder exceptions are not supported for Tamper Protection.</p> <p><a href="#">Creating a Tamper Protection exception on Windows clients</a></p>
Allow applications to make DNS or host file changes	<p>Supported on Windows clients.</p> <p>You can create an exception for an application to make a DNS or host file change. SONAR typically prevents system changes like DNS or host file changes. You might need to make an exception for a VPN application, for example.</p> <p><a href="#">Creating an exception for an application that makes a DNS or host file change</a></p>
Exclude a certificate	<p>Supported on Windows clients (starting in 14.0.1).</p> <p>You can exclude a certificate from scans. Excluding a certificate prevents it from being flagged as suspicious. A Download Insight scan can flag a self-signed certificate on an internal tool as suspicious, for example.</p> <p><a href="#">Excluding a certificate from scans on Windows clients</a></p>

[Managing exceptions in Symantec Endpoint Protection](#)

[Creating exceptions from log events](#)

---

## Excluding a file or a folder from scans

You add exceptions for files or folders individually. If you want to create exceptions for more than one file, repeat the procedure.

You can configure file or folder exceptions on both Windows and Mac clients. On Windows clients, file exceptions can apply to virus and spyware scans, SONAR, and application control. Folder exceptions apply to virus and spyware scans and SONAR.

1. **Option 1:** To exclude a file from scans on Windows clients, on the **Exceptions Policy** page, click **Exceptions**.

2. Under **Exceptions**, click **Add > Windows Exceptions > File**.

3. In the **Prefix variable** drop-down box, select a common folder.

Select **[NONE]** to enter the absolute path and file name.

When you select a prefix, the exception can be used on different Windows operating systems.

4. In the **File** text box, type the name of the file.

If you select a prefix variable, the path should be relative to the prefix. If you select **[NONE]**, type the full path name.

### NOTE

Paths must be denoted by using a backward slash.

5. Under **Specify the types of scans that will exclude this file**, select the type of scan (**Security Risk**, **SONAR**, or **Application control**).

You must select at least one type.

6. For security risk scans, under **Specify the type of security risk scan**, select **Auto-Protect**, **Scheduled and on-demand**, or **All Scans**.

See the help for information about why you might want to limit the exception to a specific type of security risk scan.

7. Click **OK**.

8. **Option 2:** To exclude a folder from scans on Windows clients, on the **Exceptions Policy** page, click **Exceptions**.

9. Under **Exceptions**, click **Add > Windows Exceptions > Folder**.

10. In the **Prefix variable** drop-down box, select a common folder.

Select **[NONE]** to enter the absolute path and file name.

When you select a prefix, the exception can be used on different Windows operating systems.

11. In the **Folder** text box, type the name of the folder.

If you select a prefix variable, the path should be relative to the prefix. If you select **[NONE]**, type the full path name.

### NOTE

Paths must be denoted by using a backward slash.

12. Under **Specify the type of scan that excludes this folder**, select the type of scan (**Security Risk**, **SONAR**, **Application control**, or **All**).

You must select at least one type.

13. For security risk scans, under **Specify the type of security risk scan**, select **Auto-Protect**, **Scheduled and on-demand**, or **All Scans**.

See the help for information about why you might want to limit the exception to a specific type of security risk scan.

---

14. Click **OK**.

15. **Option 3:** To exclude a file or folder from scans on Mac clients, on the **Exceptions Policy** page, click **Exceptions**.

16. Under **Exceptions**, click **Add > Mac Exceptions > Security Risk Exceptions for File or Folder**.

17. Under **Security Risk File or Folder Exception**, in the **Prefix variable** drop-down box, select a common folder.

Select **[NONE]** to enter the absolute path and file name.

18. In the **File or Folder** text box, type the name of the file or folder.

If you select a prefix variable, the path should be relative to the prefix. If you select **[NONE]**, type the full path name.

**NOTE**

Folder paths must be denoted by using a forward slash.

19. Click **OK**.

20. **Option 4:** To exclude a folder from scans on Linux clients, on the **Exceptions Policy** page, click **Exceptions**.

21. Under **Exceptions**, click **Add > Linux Exceptions**.

22. Click **Folder**.

23. In the **Add Folder Exception** dialog box, you can choose a prefix variable, type a folder name, and either include subfolders or not.

As of 14.3 RU1, the option **Also exclude subfolders** is not supported in Symantec Agent for Linux and all subdirectories are always excluded from the scans.

If you select a prefix variable, the path should be relative to the prefix. If you select **[NONE]**, type the full path name.

**NOTE**

Folder paths must be denoted by using a forward slash.

24. Specify the type of security risk scan. Select **Auto-Protect**, **Scheduled and on-demand**, or **All scans**, and then click **OK**.

[Creating exceptions for Virus and Spyware scans](#)

[Excluding file extensions from virus and spyware scans on Windows clients and Linux clients](#)

## Excluding known risks from virus and spyware scans on Windows clients

The security risks that the client software detects appear in the **Known Security Risk Exceptions** dialog box.

The known security risks list includes information about the severity of the risk.

To exclude known risks from virus and spyware scans on Windows clients

1. On the **Exceptions Policy** page, click **Exceptions**.

2. Under **Exceptions**, click **Add > Windows Exceptions > Known Risks**.

3. In the **Add Known Security Risk Exceptions** dialog box, select one or more security risks that you want to exclude from virus and spyware scans.

4. Check **Log when the security risk is detected** if you want to log the detection.

If you do not check this option, the client ignores the risk when it detects the selected risks. The client therefore does not log the detection.

- 
5. Click **OK**.
  6. If you are finished with the configuration for this policy, click **OK**.

#### [Creating exceptions for Virus and Spyware scans](#)

### **Excluding file extensions from virus and spyware scans on Windows clients and Linux clients**

You can add multiple file extensions to an exception. After you create the exception, you cannot create another extensions exception for the same policy. You must edit the existing exception.

You can add only one extension at a time. If you enter multiple extension names in the **Add** text box, the policy treats the entry as a single extension name.

#### [Creating exceptions for Virus and Spyware scans](#)

To exclude file extensions from virus and spyware scans on Windows clients and Linux clients

1. On the **Exceptions Policy** page, click **Exceptions**.
2. Under **Exceptions**, click **Add > Windows Exceptions > Extensions** or **Add > Linux Exceptions > Extensions**.
3. In the text box, type the extension that you want to exclude, and then click **Add**.
4. Under **Specify the type of security risk scan**, select **Auto-Protect**, **Scheduled and on-demand**, or **All Scans**.
5. Add any other extensions to the exception.
6. Click **OK**.

#### [Excluding a file or a folder from scans](#)

### **Monitoring an application to create an exception for the application on Windows clients**

When Symantec Endpoint Protection learns a monitored application, the application appears in the **Application Exception** dialog. You can create an exception action for the application in the Exceptions policy. The application also appears in the relevant log, and you can create an exception from the log.

If you disable application learning, the Application to Monitor exception forces application learning for the specified application.

To monitor an application to create an exception for the application on Windows clients

1. On the **Exceptions Policy** page, click **Exceptions**.
2. Click **Add > Windows Exceptions > Application to Monitor**.
3. In the dialog box, type the application name.

For example, you might type the name of an executable file as follows:

```
foo.exe
```

4. Click **Add**.
5. Click **OK**.

#### [Monitoring the applications and services that run on client computers](#)

#### [Creating exceptions for Virus and Spyware scans](#)

#### [Specifying how Symantec Endpoint Protection handles monitored applications on Windows clients](#)

#### [Creating exceptions from log events](#)

---

## Specifying how Symantec Endpoint Protection handles monitored applications on Windows clients

You can monitor a particular application so that you can create an exception for how Symantec Endpoint Protection handles the application. After Symantec Endpoint Protection learns the application and the management console receives the event, the application appears in the application list in the **Application Exception** dialog. The application list appears empty if the client computers in your network have not yet learned any applications.

The applications list includes the applications that you monitor as well as the files that your users download. Symantec Endpoint Protection applies the action when either Symantec Endpoint Protection detects the application or the application runs.

The applications also appear in the list for **DNS and Host File Change Exception**.

To specify how Symantec Endpoint Protection handles monitored applications on Windows clients

1. On the **Exceptions Policy** page, click **Exceptions**.
2. Click **Add > Windows Exceptions > Application**.
3. In the **View** drop-down box, select **All**, **Watched Applications**, or **User-allowed Applications**.
4. Select the applications for which you want to create an exception.
5. In the **Action** drop-down box, select **Ignore**, **Log only**, **Quarantine**, **Terminate**, or **Remove**.

The **Ignore** and **Log only** actions apply when scans detect the application as bad or malicious. The **Terminate**, **Quarantine**, and **Remove** actions apply when the application launches.

6. Click **OK**.

[Monitoring an application to create an exception for the application on Windows clients](#)

[Creating exceptions for Virus and Spyware scans](#)

[Monitoring the applications and services that run on client computers](#)

[Creating an exception for an application that makes a DNS or host file change](#)

## Excluding a trusted web domain from scans on Windows clients

You can exclude a web domain from virus and spyware scans and from SONAR. When you exclude a trusted web domain, any file that the user downloads from any location within that domain is always allowed. However, Auto-Protect and other defined scans still scan the file.

By default, Download Insight excludes the websites that appear on the **Internet Trusted Sites** list through **Internet Explorer > Tools > Internet Options > Security**. You can configure this setting from the Download Insight settings in the **Virus and Spyware Protection** policy.

If Download Insight or Auto-Protect is disabled, trusted web domain exceptions are also disabled.

### NOTE

You should use caution when you configure exceptions. Every exception that you create lowers the security profile of the computer. Consider submitting any suspected false positives for examination rather than opening a permanent scan exclusion. Always use the multiple layers of protection that Symantec Endpoint Protection provides.

[Report a Suspected Erroneous Detection \(False Positive\)](#)

## Supported web domain exceptions

Follow these guidelines when you create a web domain exception:

- 
- You must enter a single domain as a URL or an IP address when you specify a trusted web domain exception. You can specify only one domain at a time.
  - Port numbers are not supported.
  - When you specify a URL, the exception uses only the domain name portion of a URL. You can prepend the URL with either HTTP or HTTPS (case-insensitive), but the exception applies to both protocols.
  - When you specify an IP address, the exception applies to both the specified IP address and its corresponding host name. If a user navigates to a location through its URL, Symantec Endpoint Protection resolves the host name to the IP address and applies the exception. You can prepend the IP address only with HTTP (case-insensitive).
  - Both Download Insight and SONAR exclude the domain regardless of whether a user navigates to the domain through HTTP or HTTPS.
  - For an FTP location, you must specify an IP address. FTP URLs are not supported.
  - The wildcard \* is supported for use with exceptions for trusted web domains.
  - URL reputation in the Intrusion Prevention policy allows any websites that you specify as a Trusted Web Domain Exception.

To exclude a trusted web domain from scans on Windows clients

1. On the **Exceptions Policy** page, click **Add > Windows Exceptions > Trusted Web Domain**.
2. In the **Add Trusted Web Domain Exception** dialog box, enter the domain name or IP address that you want to exclude.

[Guidelines for web domain exceptions](#)

3. Click **OK**.
4. Repeat the procedure to add more web domain exceptions.

[Creating exceptions for Virus and Spyware scans](#)

## Creating a Tamper Protection exception on Windows clients

You can create file exceptions for Tamper Protection. You might want to create a Tamper Protection exception if Tamper Protection interferes with a known safe application on your client computers. For example, Tamper Protection might block an assistive technology application, such as a screen reader.

You need to know the name of the file that is associated with the assistive technology application. Then you can create an exception to allow the application to run.

### NOTE

Tamper Protection does not support folder exceptions.

14.2 RU1 and later includes support for the **[User Profile]** and **[System]** prefix variables.

To create Tamper Protection exception on Windows clients

1. On the **Exceptions Policy** page, click **Exceptions**.
2. Click **Add > Windows Exceptions > Tamper Protection Exception**.
3. In the **Add Tamper Protection Exception** dialog box, in the **Prefix variable** drop-down box, select a common folder.  
When you select a prefix, the exception can be used on different Windows operating systems.  
Select **[NONE]** if you want to enter the absolute path and file name.
4. In the **File** text box, type the name of the file.

If you selected a prefix, the path should be relative to the prefix. If you selected **[NONE]** for the prefix, type the full path name.

---

You must specify a file name. Tamper Protection does not support folder exceptions. If you enter a folder name, Tamper Protection does not exclude all the files in a folder with that name. It only excludes a file with that specified name.

5. Click **OK**.

#### [Creating exceptions for Virus and Spyware scans](#)

### **Creating an exception for an application that makes a DNS or host file change**

You can create an exception for a specific application that makes a DNS or host file change. SONAR might prevent system changes like DNS or host file changes. You might need to make an exception for a VPN application, for example.

You can monitor a particular application so that you can create a DNS or host file change exception. After Symantec Endpoint Protection learns the application and the management console receives the event, the application appears in the application list. The application list appears empty if the client computers in your network have not yet learned any applications.

Use the SONAR settings to control how SONAR detects DNS or host file changes globally.

To create an exception for an application that makes a DNS or host file change

1. On the **Exceptions Policy** page, click **Exceptions**.
2. Click **Add > Windows Exceptions > DNS or Host File Change Exception**.
3. Select the applications for which you want to create an exception.
4. In the **Action** drop-down box, select **Ignore**, **Log only**, **Prompt**, or **Block**.

The actions apply when scans detect the application making a DNS or host file change.

5. Click **OK**.

#### [Creating exceptions for Virus and Spyware scans](#)

#### [Specifying how Symantec Endpoint Protection handles monitored applications on Windows clients](#)

#### [Adjusting SONAR settings on your client computers](#)

### **Excluding a certificate from scans on Windows clients**

As of 14.0.1, you can add exceptions for certificates individually to prevent the files that it signs from being scanned and detected as suspicious. For example, a tool that your company developed internally may use a self-signed certificate. Excluding this certificate from scans prevents Auto-Protect, Download Insight, SONAR, or other scans from detecting the files that it signs as suspicious.

The certificate exclusion supports the X.509 and base64 certificate types only. When you add a certificate exception, you need a copy of the public certificate in a DER or base64 encoded file (.cer).

Certificate exclusions are not supported for the following items:

- Memory Exploit Mitigation
- Proactive Threat Protection system change events
- Tamper Protection
- Certificate-signed files within a compressed file

The excluded certificate does not have to be installed in the certificate store on the client computer in order for the exclusion to work. In the case of a conflict between a certificate exception and a deny list rule, the deny list rule takes precedence.

---

You can only add a certificate exception through the Symantec Endpoint Protection Manager policy, not through the Symantec Endpoint Protection client interface settings.

#### NOTE

You can only add a certificate exception in Symantec Endpoint Protection Manager if it is unenrolled from the cloud console. If Symantec Endpoint Protection Manager is enrolled, use the cloud console to add or manage a certificate exception.

To exclude a certificate from scans on Windows clients

1. On the **Exceptions Policy** page, click **Exceptions**.
2. Under **Exceptions**, click **Add > Windows Exceptions > Certificate**.

If Symantec Endpoint Protection Manager is enrolled in the cloud console, this option does not appear. Instead, add certificate exceptions in the cloud console.

3. Under **Certificate File**, click **Browse** to navigate to the certificate that you want to exclude, and then click **OK**.
4. Confirm that the values under **Certificate Information** are correct for the certificate that you want to exclude, and then click **OK**.

To create exceptions for more than one certificate, repeat the procedure.

#### [Creating exceptions for Virus and Spyware scans](#)

### Restricting the types of exceptions that users can configure on client computers

You can configure restrictions so that users on client computers cannot create exceptions for virus and spyware scans or for SONAR. By default, users are permitted to configure exceptions.

Users on client computers can never create exceptions for Tamper Protection, regardless of the restriction settings.

Users also cannot create file exceptions for application control.

To restrict the types of exceptions that users can configure on client computers

1. On the **Exceptions Policy** page, click **Client Restrictions**.
2. Under **Client Restrictions**, uncheck any exception that you do not want users on client computers to configure.
3. If you are finished with the configuration for this policy, click **OK**.

#### [Managing exceptions in Symantec Endpoint Protection](#)

### Creating exceptions from log events

You can create exceptions from log events for virus and spyware scans, SONAR, application control, and Tamper Protection.

#### NOTE

You cannot create exceptions from log events for early launch anti-malware detections.

**Table 130: Exceptions and log types**

Exception Type	Log Type
File	Risk log
Folder	Risk log SONAR log



Exception Type	Log Type
Known risk	Risk log
Extension	Risk log
Application	Risk log SONAR log
Trusted Web domain	Risk log SONAR log
Tamper Protection	Application Control log
DNS or host file change	SONAR log

Symantec Endpoint Protection must have already detected the item for which you want to create an exception. When you use a log event to create an exception, you specify the Exceptions policy that should include the exception.

To create exceptions from log events

1. On the **Monitors** tab, click the **Logs** tab.
2. In the **Log type** drop-down list, select the Risk log, SONAR log, or Application and Device Control log.
3. If you selected Application and Device Control, select **Application Control** from the **Log content** list.
4. Click **View Log**.
5. Next to **Time range**, select the time interval to filter the log.
6. Select the entry or entries for which you want to create an exception.
7. Next to **Action**, select the type of exception that you want to create.

The exception type that you select must be valid for the item or items that you selected.

8. Click **Apply** or **Start**.
9. In the dialog box, remove any items that you do not want to include in the exception.
10. For security risks, check **Log when the security risk is detected** if you want Symantec Endpoint Protection to log the detection.
11. Select all of the Exceptions policies that should use the exception.
12. Click **OK**.

[Monitoring endpoint protection](#)

[Managing exceptions in Symantec Endpoint Protection](#)

[Creating exceptions for Virus and Spyware scans](#)

## Configuring Web and Cloud Access Protection

The Web and Cloud Access Protection policy integrates Symantec Web Security Service (WSS) functionality into Symantec Endpoint Protection. Web and Cloud Access Protection automatically redirects all Internet traffic or just web traffic on the client to the Symantec WSS, where the traffic is allowed or blocked based on the WSS policies.

[What is Web and Cloud Access Protection?](#)

To use this feature in Symantec Endpoint Protection Manager (SEPM), you must have a valid Symantec Web Security Service subscription. Contact your account representative for a subscription.

## NOTE

In 14.3 RU2, Network Traffic Redirection was renamed to Web and Cloud Access Protection. In 14.3 RU1, WSS Traffic Redirection was renamed to Network Traffic Redirection and the Integrations policy was renamed to the Network Traffic Redirection policy.

## Technical requirements and limitations

Requirement	Description
<b>Supported Browsers</b>	<p><i>Windows:</i></p> <ul style="list-style-type: none"><li>• Microsoft Internet Explorer 9 - 11</li><li>• Mozilla Firefox</li><li>• Google Chrome</li><li>• Microsoft Edge</li></ul> <p><i>Mac:</i></p> <ul style="list-style-type: none"><li>• Macs support Apple Safari, Google Chrome, and Mozilla Firefox.</li><li>• Firefox versions 65 and later are supported in 14.2 RU1 or later.</li></ul>
<b>Limitations</b>	<ul style="list-style-type: none"><li>• The Web Security Service is delivered on IPv4 and not IPv6.</li><li>• If the Web and Cloud Access Protection feature is installed on an endpoint, the standalone Symantec WSS Agent (WSSA) cannot be installed. Similarly, if WSSA is installed, the Web and Cloud Access Protection feature does not install. However, you can remove Web and Cloud Access Protection from existing endpoints without having to uninstall the whole client by using one of the following methods:<ul style="list-style-type: none"><li>– In Symantec Endpoint Protection Manager, create a Client Install Feature Set that does not include Web and Cloud Access Protection and apply it to the endpoints. <a href="#">Add or remove features to existing Endpoint Protection clients</a></li><li>– The following command line option uses the client installation file to remove Web and Cloud Access Protection: <code>setup.exe /s /v" REMOVE=NTR /qn"</code></li></ul></li></ul> <p>The tunnel method has the following limitations:</p> <ul style="list-style-type: none"><li>• Runs on Windows 10 64-bit version 1703 and later (Semi-Annual Servicing Channel) only. This method does not support any other Windows operating systems or the Mac client.</li><li>• The Long-Term Servicing Channel (LTSC) is not supported. Microsoft intends for LTSC to be used only for specialized systems.</li><li>• Does not support HVCI-enabled Windows 10 64-bit devices</li><li>• The client computer contacts ctc.symantec.com during the installation to convert the integration token to your CustomerID. If that contact can't be made, the installation fails. To avoid this possibility for all clients, you can use your CustomerID instead of the integration token so that the conversion is not necessary.</li><li>• Outbound traffic from the Symantec Endpoint Protection client is redirected to WSS before it gets evaluated by either the client's firewall or the URL reputation rules. Instead, that traffic is evaluated against the WSS firewall and the URL rules. For example, if a SEP client firewall rule blocks google.com and a WSS rule allows google.com, the client allows users to access google.com. Inbound local traffic to the client is still processed by the Symantec Endpoint Protection firewall.</li><li>• The WSS Captive Portal is not available for the tunnel method, and the client ignores the challenge credentials. In a future release, SAML authentication in the WSS agent will replace the Captive Portal, and will be available in the Symantec Endpoint Protection client.</li><li>• If a client computer connects to the WSS using the tunnel method and hosts virtual machines, each guest user needs to install the SSL certificate provided in the WSS portal.</li><li>• Traffic for local network like your home directory or Active Directory authentication is not redirected.</li><li>• It is not compatible with the Microsoft DirectAccess VPN.</li></ul>

## Configuring the Web and Cloud Access Protection policy with the PAC file method

The WSS administrator provides the Proxy Auto Configuration (PAC) file URL or the integration token from the WSS portal. You then update the Web and Cloud Access Protection policy with the PAC file or integration token, and assign the Web and Cloud Access Protection policy to a group.

---

## Connectivity: WSS-SEP-WTR With Seamless Identification

### Best practices for Endpoint Protection and Web Security Services integration

#### Configuring Web and Cloud Access Protection with the tunnel method

The tunnel method is considered an early adopter release feature. You should perform thorough testing with your applications against your WSS policies.

**Table 131: Configuring the tunnel method**

Steps	Description
Step 1: Obtain an integration token from the WSS portal	<ol style="list-style-type: none"><li>1. Add the integration token a new or default Web and Cloud Access Protection policy. <a href="#">Connectivity: WSS-SEP-NTR With Seamless Identification</a></li><li>2. Keep the policy unlocked.</li><li>3. Assign the Web and Cloud Access Protection policy to the test group.</li></ol>
Step 2: Check that Web and Cloud Access Protection is enabled on the client	While you test the client, make sure that the Web and Cloud Access Protection is enabled and connected to the WSS. You also want to make sure that the client user can disable Web and Cloud Access Protection in case a misconfigured WSS policy keeps the user from accessing a resource. <a href="#">Verifying that Web and Cloud Access Protection is enabled on the client</a>
Step 3: Configure and test WSS policies.	To test Web and Cloud Access Protection, you first set up or modify the WSS policies in a lab environment. You then run the various test scenarios against the WSS policy, which often involves comparing a device's compliance against a WSS policy. <a href="#">Testing Web and Cloud Access Protection policies on the Symantec Endpoint Protection client</a>
Step 4: Lock the Web and Cloud Access Protection policy.	After you are sure that the WSS policies work the way you expect them to on the Symantec Endpoint Protection client, lock the policy so that the client computer is protected and that the user cannot disconnect the client from the WSS. To lock Web and Cloud Access Protection, lock the padlock in the SEPM Web and Cloud Access Protection policy.

#### Reporting

- Configuration changes to the Web and Cloud Access Protection policy appear in the Symantec Endpoint Protection Manager Audit log.
- Events for the tunnel method appear in the client's Web and Cloud Access Protection log. These events get uploaded to the Symantec Endpoint Protection Manager System log.

To view the Web and Cloud Access Protection log on the client:

1. On the client computer **Status** page, next to **Web and Cloud Access Protection**, click **Options > View Logs**.

#### Version changes

- For versions 14.0.1 MP1 to 14.2 RU1, WSS Traffic Redirection applies to Windows computers only.
- In 14.2 RU2, support was added for Mac computers.
- In 14.2, support was added to allow enhanced client authentication with WSS and a more granular control of web traffic, which is based on the user who sends it.
- In 14.3 RU1, WSS Traffic Redirection was renamed to Network Traffic RedirectionWeb and Cloud Access Protection.
- In 14.3 RU1, a new connection method was added, called the tunnel method.

## What is Web and Cloud Access Protection?

Web and Cloud Access Protection protects client computers from unsafe URLs by redirecting network traffic to the Symantec Web Security Service (WSS), where the WSS policies allow or block the traffic on the Symantec Endpoint

---

Protection (SEP) client. Integration with the Symantec WSS ensures that employees cannot access malicious websites or cannot adhere to your already defined web-use policies.

### How Web and Cloud Access Protection works

The WSS administrator generates either a PAC file or an integration token in the Symantec WSS portal. You add the PAC file or the integration token to the Symantec Endpoint Protection Manager Web and Cloud Access Protection policy, which then pushes the integration out to the SEP clients. The client computer contacts [ctc.symantec.com](http://ctc.symantec.com) to convert the integration token to your CustomerID, which contains the logged-in user ID and device information. With the customer ID, users do not have to log on every time they access the Internet. When client users log on to their computers, the SEP client initiates a secure connection (with a session key and a pre-shared key (PSK)) to the WSS. The SEP client then provides an *assertion* to the WSS. The assertion contains the user identity and other information about the computer, such as the OS version. This *seamless identification* means that users do not have to log on again when they access the Internet through the Captive Portal or Roaming Captive Portal (PAC file method only). This process allows for a per-user policy to be applied to traffic and provides risky client context to the WSS for logging and reporting.

All supported browser traffic is handled in one of the following ways:

- Redirects it to the WSS server
- Blocks it
- Allows it to continue to its destination

### Redirection methods

The Network Threat Redirection policy provides two redirection methods between the client and the Symantec WSS. The following table describes the benefits of each method, and how they work.

**Table 132: Redirection methods**

Method	When to use it	How it works
<b>Tunnel</b>	<p>The tunnel method embeds and deploys the WSS agent technology into Symantec Endpoint Protection, which captures non-proxy applications. This method:</p> <ul style="list-style-type: none"> <li>• Redirects to any port, not just 80 and 443.</li> <li>• Redirects any application, not just web browsers. You can also choose to redirect just web traffic.</li> <li>• Is more robust for roaming users who change networks frequently</li> <li>• Provides better security between the client computer and the data center by encrypting traffic. The PAC file method does not encrypt traffic.</li> <li>• Is considered the primary connection method to WSS in the future.</li> <li>• Runs on Windows 10 64-bit version 1703 and later only.</li> <li>• The Windows 10 Long-Term Servicing Channel (LTSC) is not supported. Microsoft intends for LTSC to be used only for specialized systems.</li> </ul>	<p>The WSS administrator generates a randomized integration token in the WSS portal and adds it to the Web and Cloud Access Protection policy. This method captures traffic from non-proxy aware application and enables a more granular level of security management than the PAC file redirection alone. The WSS integration token forwards more header data to identify the user that initiated the traffic, allowing for per-user traffic rules.</p> <p>The traffic that is redirected through the tunnel method depends on how your WSS policies are set up. For example, the policy rules can specify web traffic only, or all ports and protocols. The tunnel method also depends on your WSS license.</p> <p>The tunnel method installs the certificate by default because it is an encrypted tunnel.</p>
<b>PAC File</b>	<p>The PAC File method:</p> <ul style="list-style-type: none"> <li>• Is faster than the tunnel method.</li> <li>• Runs on all supported Windows operating systems.</li> <li>• Runs on Mac computers.</li> <li>• Redirects web traffic only.</li> </ul>	<p>The WSS administrator configures a PAC file in the WSS portal to get a PAC file URL. The PAC file automates the web traffic redirection to the WSS and provides secure proxy settings for your web browsers. The PAC file method allows port 80 and 443 traffic (web traffic) to be redirected for inspection. However, it is unable to re-direct traffic outside of 80/443, or from applications that do not honor the proxy. Only web traffic is redirected to the WSS.</p> <p>Every time a user accesses a website using a web browser, the browser sends all web browser traffic through the nearest cloud-hosted Web Security Service as defined by the PAC file. Based on the rules that the PAC file defines, all supported browser traffic is handled in one of the following ways:</p> <ul style="list-style-type: none"> <li>• Without a WSS integration token, all web browser traffic visits the PAC file URL for WSS. All users abide by the same traffic rules for WSS.</li> <li>• With a WSS integration token, all web browser traffic visits a locally cached PAC file for WSS. WSS can determine from which user the traffic came, and direct the web traffic accordingly.</li> </ul> <p>The PAC File method was called Web Traffic Redirection (WTR) in 14.3 MP1 and earlier.</p>

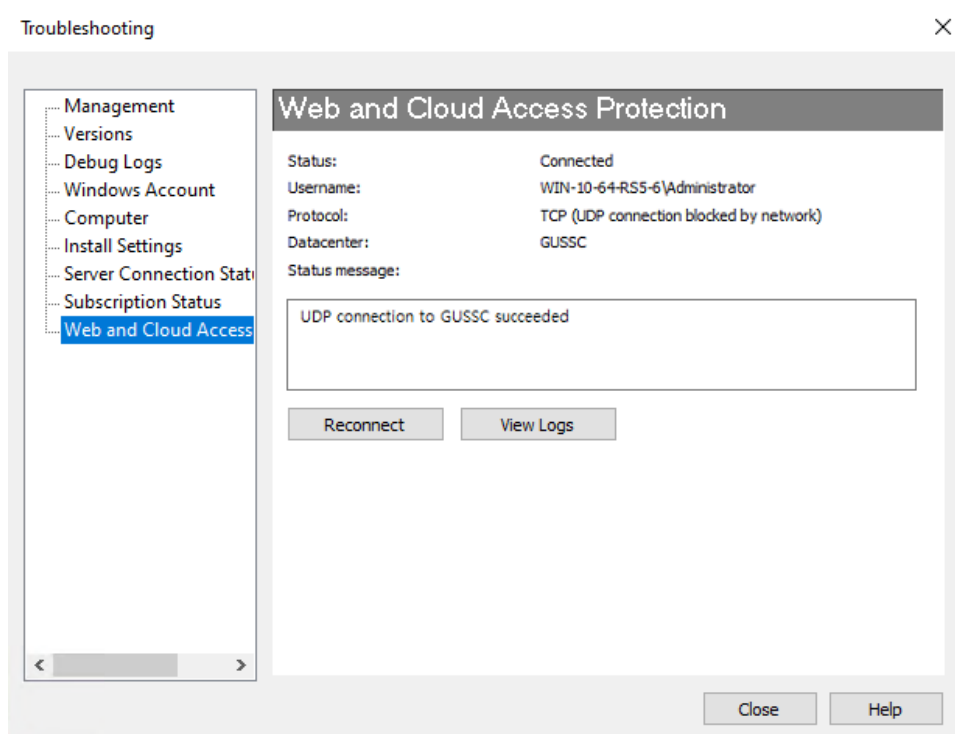
---

## Verifying that the Web and Cloud Access Protection tunnel method is enabled and connected on the client

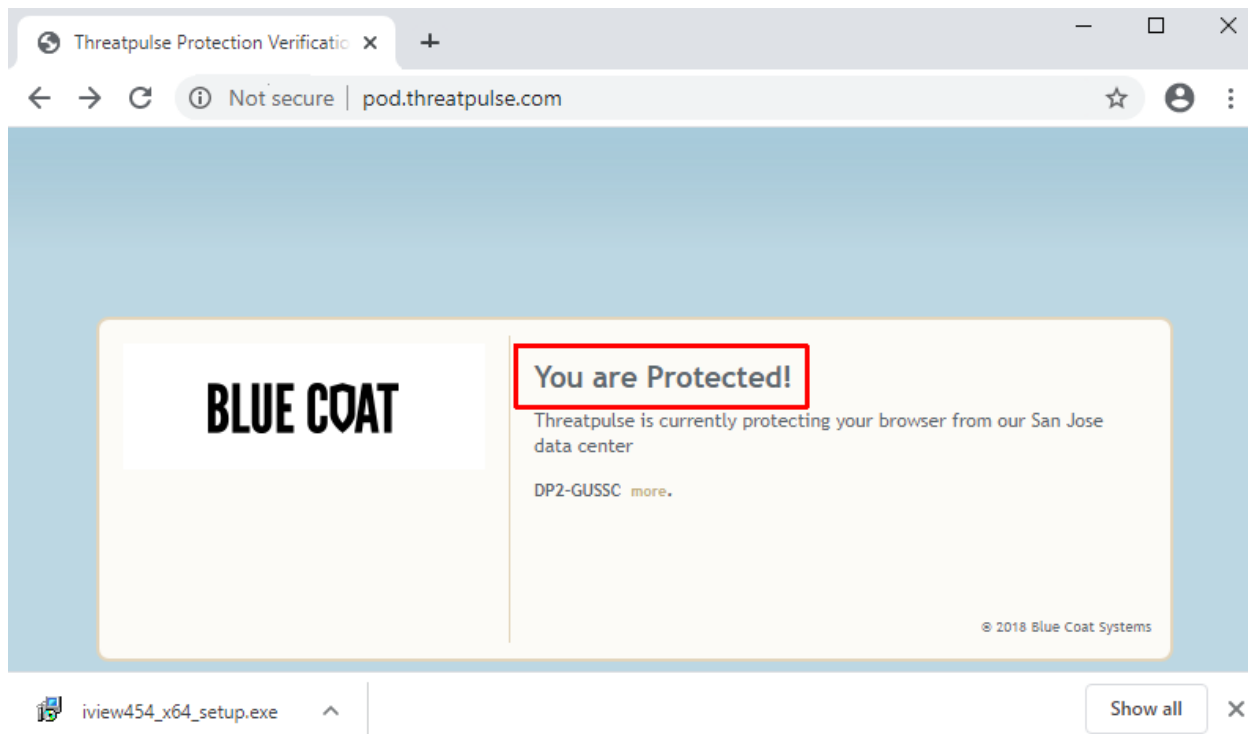
1. On the Symantec Endpoint Protection (SEP) client, click **Help > Troubleshooting > Web and Cloud Access Protection**.

If the Web and Cloud Access Protection panel appears. If the panel does not appear, the tunnel method is not enabled on the client.

Web and Cloud Access Protection is connected if the Status field displays **Connected**.




2. On the client, browse to the following test URL: `pod.threatpulse.com`.  
If Web and Cloud Access Protection is enabled, the client user should see the following message.



### Reconnecting to the WSS

Web and Cloud Access Protection should stay continually connected to the WSS. However, there are situations where the connection gets interrupted. The Wi-Fi may go down, an Internet connection gets disabled, or a data center fails. Regardless of what caused the outage, when service returns, the client user must reconnect to WSS.

You reconnect to the client based in the following situations.

Method	Description
If the client detects that the connection is broken.	<ol style="list-style-type: none"><li>1. In the SEP client, click the <b>Status</b> page.</li><li>2. At the top of the page, the stripe is green if Web and Cloud Access Protection is enabled, connected, and yellow or red if it is not.</li><li>3. To reconnect to WSS, the client user should click the <b>Fix</b> button.</li></ol> 
If the client does not detect that the connection has been broken.	<ol style="list-style-type: none"><li>1. In the client, click the <b>Status</b> page.</li><li>2. Next to <b>Web and Cloud Access Protection</b>, click <b>Options &gt; Detailed Status</b>.</li><li>3. The <b>Status</b> field should show <b>Connected</b>. If not, click <b>Reconnect</b>.</li></ol>

## Testing Web and Cloud Access Protection policies in a browser

### Visit the test websites

The WSS solution protects organizations by categorizing applications and web sites, and then allowing or denying a client user based on the WSS policy. Testing those policies is often difficult because it requires the client user to attempt to visit a site that may be dangerous, such as one categorized to have known malware. To make testing safer, Symantec has built a web site that has individual links for each category. Client users can click on a link to simulate visiting that category without risk.

1. On the client computer, open a browser window and go to <http://sitereview.symantec.com>
2. Click **Categories** and select **Test Pages**.
3. Click individual links that correspond to sites that the WSS policy allows and denies. Validate that the agent is compliant with the WSS category policy. For example, an allowed site might appear as follows:



## Test Rating

This is a Symantec WebFilter test rating page categorized as

### Charitable/Non-Profit

Sites that foster volunteerism for charitable causes. Also encompasses non-profit associations that cultivate philanthropic or relief efforts. Does not include organizations that attempt to influence legislation as a significant portion of their activities or organizations that campaign for, contribute to or affiliate with political organizations or candidates.

Examples: [scouting.org](http://scouting.org) [4-h.org](http://4-h.org) [ymca.net](http://ymca.net) [lionsclubs.org](http://lionsclubs.org) [redcross.org](http://redcross.org)  
[unicef.org](http://unicef.org) [pewtrusts.org](http://pewtrusts.org) [cityharvest.org](http://cityharvest.org) [soles4souls.org](http://soles4souls.org)

#### 4. Click **Threat Risk** and select **Test Pages**.

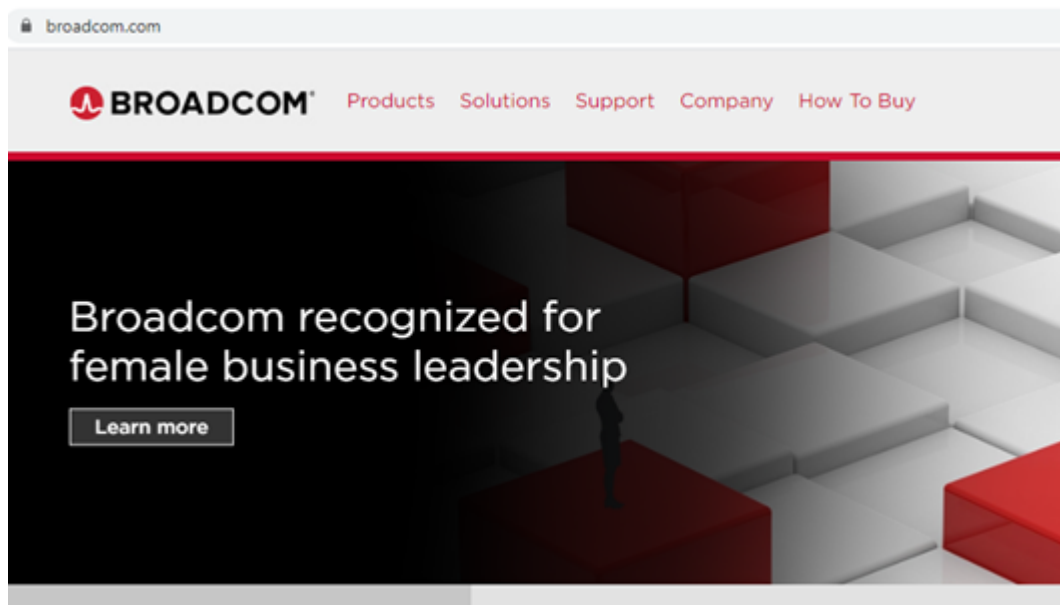
The links are sorted from 1-10 with ascending simulated risk.

#### 5. Click each link to validate that the client is compliant with the WSS risk policy.

### Visit a site allowed by policy

This example demonstrates a client user visiting a web site that the WSS policy allows. The traffic is redirected to WSS, inspected, and is passed to the web site.

1. Go to <http://www.broadcom.com>
2. Validate that the client computer opens the site.



### Test the tunnel method with WSS policies

You can test the integrated Web and Cloud Access Protection solution with the policies that the WSS administrator sets up in the WSS console. You may need to work with the WSS administrator to get a list of web sites that can be used to test each scenario, as each organization's policies are different.

---

## About Web and Cloud Access Protection for the Mac client

Web and Cloud Access Protection automates web traffic redirection to the Symantec Web Security Service and secures the web traffic on each computer that uses Symantec Endpoint Protection.

The administrator controls the settings that Web and Cloud Access Protection uses, which includes the proxy configuration URL and the optional Symantec Web Security Service root certificate. Only the Symantec Endpoint Protection Manager administrator can configure these settings, which do not appear in the Symantec Endpoint Protection client UI. You can view the proxy configuration file URL on the Mac through **System Preferences > Network**, under **Proxies**. The Cloud Services certificate appears in **Keychain**.

The web browsers Safari, Chrome, and Firefox version 65 and later support Web and Cloud Access Protection. Symantec Endpoint Protection versions earlier than 14.2 RU1 only support Safari and Chrome.

### NOTE

The tunnel method does not run on Mac clients.

## Web and Cloud Access Protection Settings

Web and Cloud Access Protection protects Windows and Mac client computers against network traffic by redirecting it to the Symantec Web Security Service (WSS), where the WSS allows or blocks the traffic. The WSS either allows or blocks the traffic based on the policy that the WSS administrator configures in the WSS.

**Note:** To use this feature within Symantec Endpoint Protection Manager, you must have a valid Web Security Service subscription. Contact your account representative for a subscription.

**Table 133: Web and Cloud Access Protection settings**

Option	Description
<b>Enable Web and Cloud Access Protection</b>	Enables or disables the Web and Cloud Access Protection feature on Symantec Endpoint Protection clients. You must check this option to enable it on the client. If you disable this option for the PAC File method, you can still enable the <b>Install the Symantec Web Security Service root certificate on clients to facilitate the protection of encrypted traffic</b> option. This option was renamed from <b>Enable WSS Traffic Redirection</b> in 14.3 RU1.
<b>Redirection Method</b>	<ul style="list-style-type: none"><li>The tunnel method automatically redirects all Internet traffic to the WSS. You should perform thorough testing with your applications against your WSS policies.</li><li>The PAC File method redirects web only traffic (ports 80 and 443).</li></ul> For information on the differences between the redirection methods, see: <a href="#">What is Web and Cloud Access Protection?</a>

**Table 134: Tunnel method options**

Option	Description
<b>Network integration token</b>	The WSS administrator generates a randomized integration token from the WSS portal. When the Symantec Endpoint Protection client receives the token, it looks up the ctc.symantec.com and converts the token to the CustomerID. The customer ID securely forwards the user ID and client-context information to the WSS after which the client connects to the WSS. <b>Note:</b> You can use the CustomerID instead of the token in cases where the client computer cannot connect to the Internet during installation.

**Table 135: PAC File method options**

Option	Description
<b>Proxy Auto Configuration (PAC) File URL</b>	Indicates the URL to the Proxy Auto Configuration file, as defined by the WSS administrator. You can configure or edit this URL in Symantec Endpoint Protection Manager only.
<b>Traffic interception port</b>	Indicates the port in use by the local proxy service. For versions earlier than 14.2 RU1, this option only applies to Windows computers.
<b>Network integration token</b>	Symantec Endpoint Protection clients use the token to securely forward user ID and client-context information to the WSS. The local proxy service requires the token to parse the header information for per-user rules to allow or block web traffic. This option allows for local caching of the PAC file. For versions earlier than 14.2 RU1, this option only applies to Windows computers.
<b>Allow direct traffic when network protection is not available</b>	Use this option to give users access to the web if user authentication with the WSS cloud proxy (proxySG) fails. This situation occurs if the administrator sets up a PAC file, but not the WSS roaming users. <ul style="list-style-type: none"> <li>If this option is checked and the client user fails to authenticate, the client fails open.</li> <li>If this option is unchecked and the client user fails to authenticate, the client fails closed.</li> </ul> Until users are authenticated, Web and Cloud Access Protection does not protect them. WSS attempts to authenticate the user every 5 minutes in the background. WSS then requests that the user to authenticate manually in the WSS Roaming Captive Portal. This setting is ignored until a valid authentication attempt is made. This option applies to clients 14.2 RU2 MP1 and later.
<b>Enable LPS Custom PAC file</b>	Replaces the default PAC file that is hosted by the LPS server on the client with a custom PAC file. The custom PAC file solves compatibility issues with third-party applications that do not work with a local proxy server listening on the loopback adapter. It is recommended that you make all other configurations for bypass and filtering through the WSS portal. This option applies to clients 14.3 and later. <b>Warning:</b> If you incorrectly configure the custom PAC file option, it can prevent client users and applications from accessing the Internet. <b>Note:</b> The effects of the custom PAC file may not take effect immediately. You may need to restart the client.
<b>Install the Symantec Web Security Service root certificate on clients to facilitate the protection of encrypted traffic</b>	Installs the appropriate root certificate on Symantec Endpoint Protection clients to protect encrypted traffic. This option can be enabled when the <b>Enable Web and Cloud Access Protection</b> option is disabled, which allows you to install root certificates even if the PAC file option is not selected.

## Testing Symantec Endpoint Protection Manager policies

You may need to evaluate Symantec Endpoint Protection or you may need to test the policies before you download them to the client computers. You can test the following functionality using the Symantec Endpoint Protection Manager policies to make sure the product works correctly on the client computers.

**Table 136: Features that you can test**

Feature	See this topic
Virus and Spyware Protection	To test a default Virus and Spyware Protection policy, download the EICAR test virus from: <a href="#">ANTI MALWARE TESTFILE</a> <a href="#">Testing a Virus and Spyware Protection policy</a>
SONAR	<a href="#">Download the Socar.exe test file to verify that SONAR works correctly</a>
Insight	<a href="#">How to test connectivity with Insight and Symantec Licensing servers</a>
Intrusion Prevention	<a href="#">Testing a default IPS policy</a>
Application Control	<a href="#">Blocking a process from starting on client computers</a> <a href="#">Preventing users from writing to the registry on client computers</a> <a href="#">Preventing users from writing to a particular file</a> <a href="#">Adding and testing a rule that blocks a DLL</a> <a href="#">Adding and testing a rule that terminates a process</a>

## Testing a Virus and Spyware Protection policy

To test to see that the Virus and Spyware policy works, you can use the test virus file eicar.com. The EICAR test virus is a text file that the European Institute for Computer Antivirus Research (EICAR) developed. It provides an easy way and safe way to test most antivirus software. You can use it to verify that the antivirus portion of the client works.

To test a Virus and Spyware Protection policy

1. On the client computer, download the antivirus test file from the EICAR website at the following location:

<http://2016.eicar.org/86-0-Intended-use.html>

2. Run the EICAR test file.

A notification appears that tells you that a risk is found.

- 
3. In Symantec Endpoint Protection Manager, on the **Monitors** page, click **Logs**.
  4. On the **Logs** tab, in the **Log type** drop-down list, click **Risk**, and then click **View Log**.
  5. On the **Risk Logs** page, the **Virus found event** appears.

## Blocking a process from starting on client computers

The FTP client is a common way to transfer files from a server to a client computer. To prevent users from transferring files, you can add a rule that blocks a user from launching an FTP client from the command prompt.

1. To add a rule that blocks a process from starting on the client computer, open an Application Control policy, and on the **Application Control** pane, click **Add**.
2. In the **Application Control Rule Set** dialog box, in the **Rules** list, select a rule, and on the **Properties** tab, in the **Rule name** text box, type `ftp_blocked_from_cmd`.
3. To the right of **Apply this rule to the following processes**, click **Add**.
4. In the **Add Process Definition** dialog box, under **Processes name to match**, type `cmd.exe`, and then click **OK**.
5. In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add Condition > Launch Process Attempts**.
6. On the **Properties** tab, in the **Description** text box, type `no ftp from cmd`.
7. To the right of **Apply this rule to the following processes**, click **Add**.
8. In the **Add Process Definition** dialog box, under **Processes name to match**, type `ftp.exe`, and then click **OK**.
9. In the **Application Control Rule Set** dialog box, on the **Actions** tab, click **Block access**, **Enable logging**, and **Notify user**.
10. Under **Notify user**, type `ftp is blocked if launched from the cmd`.
11. Click **OK** twice, and assign the policy to a group.

Test the rule.

12. To test a rule that blocks a process from starting on the client computer, on the client computer, open a command prompt.
13. In the command prompt window, type `ftp`, and then press **Enter**.

As the rule has specified, the FTP client does not open.

## Preventing users from writing to the registry on client computers

You can protect a specific registry key by preventing the user from accessing or from modifying any registry keys or values in the registry. You can allow users to view the registry key, but not rename or modify the registry key.

**To test the functionality:**

- 
- Add a test registry key.
  - Add a rule to read but not write to the registry key.
  - Try to add a new value to the registry key.
1. To add a test registry key, on the client computer, open the Registry Editor by opening a command line, then by typing `regedit`.
  2. In the Registry Editor, expand `HKEY_LOCAL_MACHINE\Software`, and then create a new registry key called `test`.
  3. To prevent users from writing to the registry on client computers, open an Application Control policy, and on the **Application Control** pane, click **Add**.
  4. In the **Application Control Rule Set**, under the **Rules** list, click **Add > Add Rule**.
  5. On the **Properties** tab, in the **Rule name** text box, type `HKLM_write_not_allowed_from_regedit`.
  6. To the right of **Apply this rule to the following processes**, click **Add**.
  7. In the **Add Process Definition** dialog box, under **Process name to match**, type `regedit.exe`, and then click **OK**.
  8. In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add > Add Condition > Registry Access Attempts**.
  9. On the **Properties** tab, in the **Description** text box, type `registry access`.
  10. To the right of **Apply this rule to the following processes**, click **Add**.
  11. In the **Add Registry Key Definition** dialog box, in the **Registry key** text box, type `HKEY_LOCAL_MACHINE\software\test`, and then click **OK**.
  12. In the **Application Control Rule Set** dialog box, on the **Actions** tab, in the **Read Attempt** group box, click **Allow access**, **Enable logging**, and **Notify user**.
  13. Under **Notify user**, type `reading is allowed`.
  14. In the **Create, Delete, or Write Attempt** group box, click **Block access**, **Enable logging**, and **Notify user**.
  15. Under **Notify user**, type `writing is blocked`.
  16. Click **OK** twice, and assign the policy to a group.  
Test the rule.
  17. To test a rule that blocks you from writing to the registry, after you have applied the policy, on the client computer, in the Registry Editor, expand `HKEY_LOCAL_MACHINE\Software`.
  18. Click the registry key that you created earlier, called `test`.
  19. Right-click the test key, click **New**, and then click **String Value**.  
You should not be able to add a new value to the test registry key.

## Preventing users from writing to a particular file

You may want users to view but not modify a file. For example, a file may include the financial data that employees should view but not edit.

---

You can create an Application and Device Control rule to give users read-only access to a file. For example, you can add a rule that lets you open a text file in Notepad but does not let you edit it.

1. To add a rule that prevents users from writing to a particular file, open an Application Control policy, and on the **Application Control** pane, click **Add**.
2. In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add > Add Rule**.
3. On the **Properties** tab, in the **Rule name** text box, type `1.txt in c read allowed write terminate`.
4. To the right of **Apply this rule to the following processes**, click **Add**.
5. In the **Add Process Definition** dialog box, under **Processes name to match**, type `notepad.exe`, and then click **OK**.
6. In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add > Add Condition > File and Folder Access Attempts**.
7. On the **Properties** tab, in the **Description** text box, type `file access launched`.
8. To the right of **Apply this rule to the following processes**, click **Add**.
9. In the **Add File or Folder Definition** dialog box, in the text box in the **File or Folder Name To Match** group box, type `c:\1.txt`, and then click **OK**.
10. In the **Application Control Rule Set** dialog box, on the **Actions** tab, in the **Read Attempt** group box, select **Allow access**, and then check **Enable logging** and **Notify user**.
11. Under **Notify user**, type `reading is allowed`.
12. In the **Create, Delete, or Write Attempt** group box, click **Block access**, **Enable logging**, and **Notify user**.
13. Under **Notify user**, type `writing to block Notepad`.
14. Click **OK** twice and assign the policy to the client computer group.

Test the rule.

15. To test a rule that prevents users from writing to a particular file, on the client computer, open File Explorer, locate the `c:\` drive, and then click **File > New > Text Document**.

If you create the file by using Notepad, the file is a read-only file.

16. Rename the file as `1.txt`.

Make sure that the file is saved to the `c:\` folder.

17. In Notepad, open the `c:\1.txt` file.

You can open the file but you cannot edit it.

## Adding and testing a rule that blocks a DLL

You may want to prevent the user from opening a specific application. One way to block a user from opening an application is to block a DLL that the application uses to run. To block the DLL, you can create a rule that blocks the DLL from loading. When the user tries to open the application, they cannot.

For example, the `Msvcr7.dll` file contains the program code that is used to run various Windows applications such as Microsoft WordPad. If you add a rule that blocks `Msvcr7.dll` on the client computer, you cannot open Microsoft WordPad

---

## NOTE

Some applications that are written to be "security conscious" may interpret the DLL injection as a malicious act. Take counter measures to block the injection or remove the DLL.

1. To add a rule that blocks a DLL, open an Application Control policy, and on the **Application Control** pane, click **Add**.
2. In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add > Add Rule**.
3. On the **Properties** tab, in the **Rule name** text box, type `Block user from opening Microsoft WordPad`.
4. To the right of **Apply this rule to the following processes**, click **Add**.
5. In the **Add Process Definition** dialog box, under **Processes name to match**, type `C:\Program Files\Windows NT\Accessories\wordpad.exe`, and then click **OK**.
6. In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add > Add Condition > Load DLL Attempts**.
7. On the **Properties** tab, in the **Description** text box, type `dll blocked`.
8. To the right of **Apply to the following DLLs**, click **Add**.
9. In the **Add DLL Definition** dialog box, in the text box in the **DLL name to match** group box, type `MSVCRT.dll`, and then click **OK**.
10. In the **Application Control Rule Set** dialog box, on the **Actions** tab, click **Block access**, **Enable logging**, and **Notify user**.
11. Under **Notify user**, type `Should not be able to load WordPad`.
12. Click **OK** twice and assign the policy to the client computer group.

Test the rule.



---

13. To test a rule that blocks a DLL, on the client computer, try to open Microsoft WordPad.

## Adding and testing a rule that terminates a process

Process Explorer is a tool that displays the DLL processes that have opened or loaded, and what resources the processes use. You can also use the Process Explorer to terminate a process. You can add a rule to terminate the Process Explorer if the user uses Process Explorer to try to terminate the Calculator application.

1. To add a rule that terminates a process, open an Application Control policy, and on the **Application Control** pane, click **Add**.
2. In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add > Add Rule**.
3. On the **Properties** tab, in the **Rule name** text box, type `Terminates Process Explorer if Process Explorer tries to terminate calc.exe`.
4. To the right of **Apply this rule to the following processes**, click **Add**.
5. In the **Add Process Definition** dialog box, under **Processes name to match**, type `procexp.exe`, and then click **OK**.
6. In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add > Add Condition > Terminate Process Attempts**.
7. On the **Properties** tab, in the **Description** text box, type `dll stopped`.
8. To the right of **Apply this rule to the following processes**, click **Add**.
9. In the **Add Process Definition** dialog box, in the text box in the **Process name to match** group box, type `calc.exe`, and then click **OK**.
10. In the **Application Control Rule Set** dialog box, on the **Actions** tab, click **Terminate process**, **Enable logging**, and **Notify user**.
11. Under **Notify user**, type `If you try to terminate the calc from procexp, procexp terminates`.
12. Click **OK** twice, and assign the policy to a group.

Test the rule.

13. To test a rule that terminates a process, on the client computer, download and run a free version of the Process Explorer from the following URL:

<http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>

14. In Windows, open the Calculator.
15. Open the Process Explorer.
16. In the **Process Explorer** window, right-click the `calc.exe` process, and then click **Kill Process**.

The Process Explorer is terminated.

## Testing a default IPS policy

To test the default IPS policy, you must first trigger an event on the client computer.

To test a default IPS policy

- 
1. Rename an executable file (.exe) to a jpeg (.jpg).
  2. Upload the .jpg file to a web server\site.
  3. On the client computer, use a web browser to open the renamed executable file.

**NOTE**

To open the renamed executable file, you must access the web server\site using the IP address. For example, you would type: `http://web server IP address/renamed executable.jpg`

4. On the client, if the IPS policy works correctly, the following events occur:
  - You should not be able to open the .jpg file.
  - A message in the notification area icon states that the client blocked the .jpg file.
  - You can open the Security log and look for a log entry that states that the client blocked the .jpg file.

---

## How to update content and definitions on the clients

---

By default, the Symantec Endpoint Protection Manager downloads content updates from the public Symantec LiveUpdate servers. Symantec Endpoint Protection clients then download these updates from the Symantec Endpoint Protection Manager. The content includes virus definitions, intrusion prevention signatures, and Host Integrity templates, among others.

**Table 137: Steps to update content on the Symantec Endpoint Protection clients**

Task	Description
Make sure that the management server has the latest content from LiveUpdate (Recommended)	<p>By default, LiveUpdate runs as part of the Symantec Endpoint Protection Manager installation. You may need to run LiveUpdate manually in the following situations:</p> <ul style="list-style-type: none"><li>• You skipped LiveUpdate during installation.</li><li>• You must run LiveUpdate to download the Host Integrity templates and intrusion prevention signatures.</li><li>• You want to run LiveUpdate before the next scheduled update.</li></ul> <p><a href="#">Checking that Symantec Endpoint Protection Manager has the latest content</a></p> <p>You can also update content on Symantec Endpoint Protection Manager with a .jdb file.</p> <p><a href="#">Download .jdb files to update definitions for Endpoint Protection Manager</a></p> <p>Additionally, if you use replication, you can replicate content and policies between the local site and the partner site.</p> <p><a href="#">How to install a second site for replication</a></p>
Change how client computers get updates (Optional)	<p>By default, Windows client computers get content updates from the management server. Other delivery methods include Group Update Providers, internal LiveUpdate servers, or third-party tool distribution. You may need to change the delivery method to support different client platforms, large numbers of clients, or network limitations.</p> <p><a href="#">Choose a distribution method to update content on clients</a></p> <p><a href="#">Choose a distribution method to update content on clients based on the platform</a></p>
Change the LiveUpdate settings for the management server (Optional)	<p>You can customize the frequency of LiveUpdate sessions, the protection components that are downloaded, and more.</p> <p><a href="#">Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager</a></p>
Reduce network overloads (Recommended)	<p>If the management server receives too many concurrent requests for full definition packages from the clients, the network may become overloaded. You can mitigate the risk of these overloads, and stop clients from downloading full definitions.</p> <p><a href="#">Mitigating network overloads for client update requests</a></p>
Improve performance (Recommended)	<p>To help mitigate the effect of downloads on network bandwidth, download content randomly so that not all clients get updates at the same time.</p> <p><a href="#">About randomization of simultaneous content downloads</a></p> <p><a href="#">Randomizing content downloads from the default management server or a Group Update Provider</a></p> <p><a href="#">Randomizing content downloads from a LiveUpdate server</a></p> <p>To mitigate the effect of downloads on client computers' performance, you can have the client computers download content updates when the client computers are idle.</p> <p><a href="#">Configuring Windows client updates to run when client computers are idle</a></p>
Let your endpoint users manage their own updates (Optional)	<p>By default, users on the client computer can run LiveUpdate at any time. You can decide how much control to give your users over their content updates.</p> <p><a href="#">Configuring the amount of control that users have over LiveUpdate</a></p> <p>You can also use an Intelligent Updater file on a client computer to update the definitions.</p> <p><a href="#">Using Intelligent Updater files to update content on Symantec Endpoint Protection clients</a></p>

Task	Description
Test engine updates before Symantec releases them (Optional)	Symantec releases engine updates on a quarterly basis. You can download the engine updates before they are released using a specific Symantec LiveUpdate server. You can then test the engine content before you roll out the content to your production environment. <a href="#">Testing engine updates before they release on Windows clients</a>

## Choose a distribution method to update content on clients

You may need to change the default update method to the clients, depending on the client platform, network configuration, number of clients, or your company's security policies and access policies.

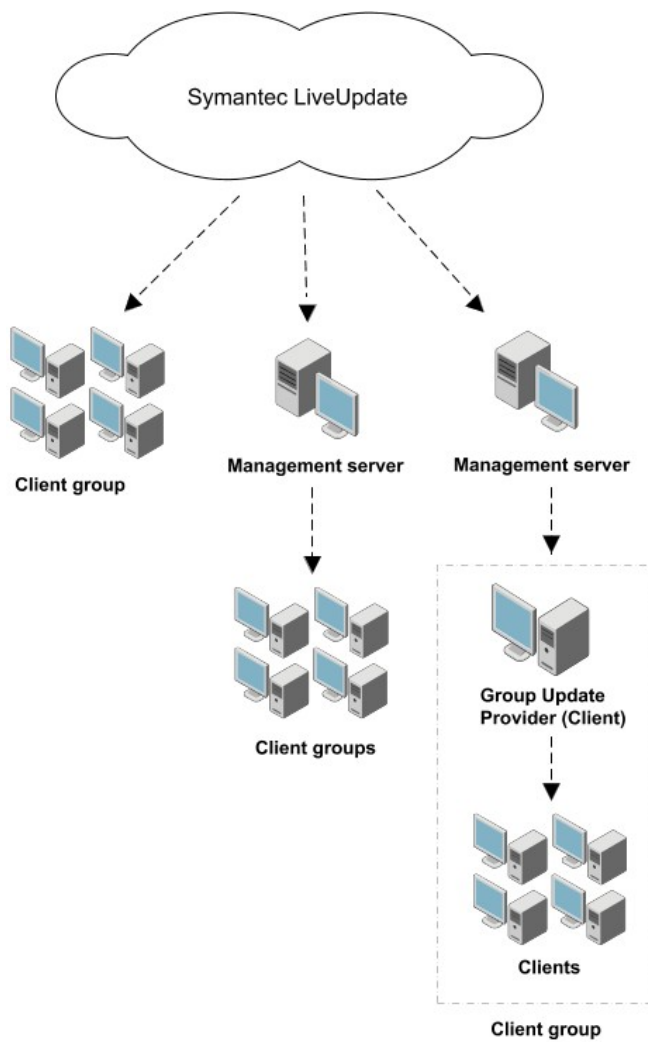
**Table 138: Content distribution methods and when to use them**

Method	Description	When to use it
Symantec Endpoint Protection Manager to client computers (default) (Windows, Mac, Linux)	The default management server automatically updates the client computers that it manages. You do not define the schedule for the updates from the management server to the clients. The clients download content from the management server based on the communication mode and heartbeat frequency. <a href="#">Configuring clients to download content from the Symantec Endpoint Protection Manager</a> <a href="#">Updating policies and content on the client using push mode or pull mode</a>	Symantec recommends that you use this method unless network constraints or your company's policies require an alternative. If you have a large number of clients or bandwidth issues, you might use this method, along with Group Update Providers. For Mac or Linux computers to receive content updates from the management server, you must configure the Apache web server. <a href="#">Enabling Mac and Linux clients to download LiveUpdate content using the Apache Web server as a reverse proxy</a>
Group Update Provider to client computers (Windows only)	A Group Update Provider is a client computer that receives updates from a management server. The Group Update Provider then forwards the updates to the other client computers in the group. A Group Update Provider can update multiple groups. Group Update Providers can distribute all types of LiveUpdate content except client software updates. Group Update Providers also cannot be used to update policies.	A Group Update Provider lets you reduce the load on the management server, and is easier to configure than an internal LiveUpdate server. Use a Group Update Provider for groups at remote locations with minimal bandwidth. <a href="#">Using Group Update Providers to distribute content to clients</a> <a href="#">Deciding whether or not to set up multiple sites and replication</a>

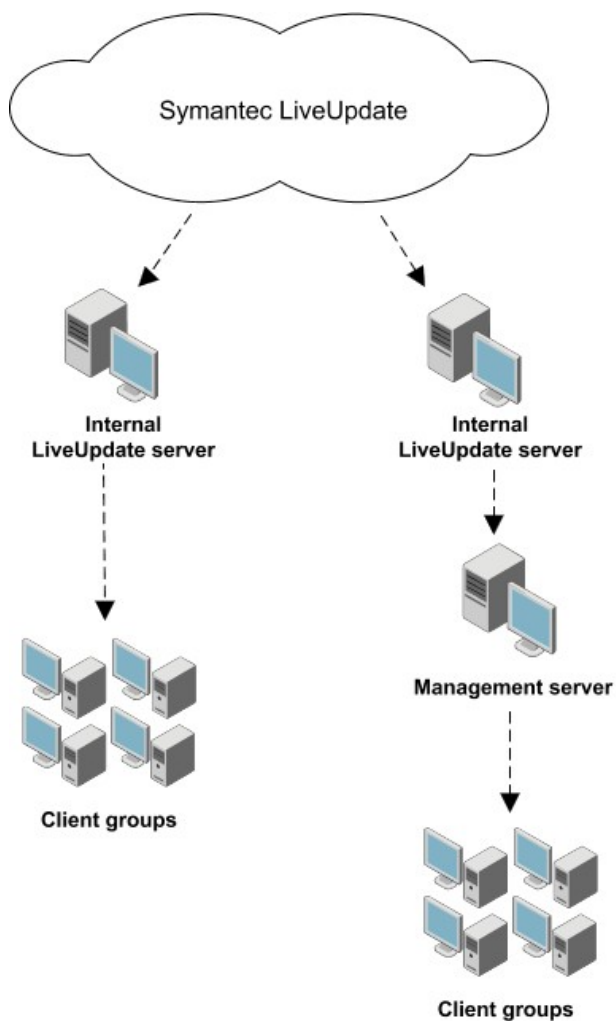
Method	Description	When to use it
Internal LiveUpdate server to client computers (Windows, Mac, Linux)	<p>Client computers can download updates directly from an internal LiveUpdate server that receives its updates from a Symantec LiveUpdate server.</p> <p>If necessary, you can set up several internal LiveUpdate servers and distribute the list to client computers.</p> <p>You can change the download schedule from the LiveUpdate server to the management server.</p> <p><a href="#">Configuring the LiveUpdate download schedule to client computers</a></p> <p>For more information about setting up an internal LiveUpdate server, see the <i>LiveUpdate Administrator User's Guide</i> at:  <a href="#">Downloading LiveUpdate Administrator</a></p>	<p>An internal LiveUpdate server lets you reduce the load on the management server in very large networks. In smaller networks, consider whether Group Update Providers would meet your organization's needs. Consider using an internal LiveUpdate server in the following situations:</p> <ul style="list-style-type: none"> <li>• If you manage a large network (more than 10,000 clients)</li> <li>• If you manage Mac or Linux clients that should not connect to an external LiveUpdate server</li> <li>• If your organization deploys multiple Symantec products that also use LiveUpdate to distribute content to client computers</li> </ul> <p><b>Note:</b> You should not install the management server and an internal LiveUpdate server on the same physical hardware or virtual machine. Installation on the same computer can result in significant server performance problems.</p> <p>For more information see:  <a href="#">LiveUpdate Administrator 2.x and Symantec Endpoint Protection Manager on the same computer</a>  <a href="#">Configuring clients to download content from an internal LiveUpdate server</a></p>
External Symantec LiveUpdate server to client computers over the Internet (Windows, Mac, Linux)	<p>Client computers can receive updates directly from a Symantec LiveUpdate server.</p>	<p>Use an external Symantec LiveUpdate server if you need to schedule when clients update content or if the available bandwidth between the Symantec Endpoint Protection Manager and the clients is limited. Symantec Endpoint Protection Manager and scheduled updates are enabled by default. With the default settings, clients always get updates from the management server unless management server is unresponsive for a long period of time.</p> <p><b>Note:</b> Do not configure large numbers of managed, networked clients to pull updates from an external Symantec LiveUpdate server. This configuration consumes unnecessary bandwidth.</p> <p><a href="#">Configuring clients to download content from an external LiveUpdate server</a></p>
Third-party tool distribution (Windows only)	<p>Third-party tools like Microsoft SMS let you distribute specific update files to clients.</p>	<p>This method lets you test update files before you distribute them. It may also make sense if you have a third-party tool distribution infrastructure in place.</p> <p><a href="#">Distributing the content using third-party distribution tools</a></p>
Intelligent Updater (Windows only)	<p>Intelligent Updater files contain the virus and security risk content and intrusion prevention content that you can use to manually update clients.</p> <p>You can download the Intelligent Updater self-extracting files from the Symantec Web site.</p>	<p>You can use Intelligent Updater files if LiveUpdate is not available.</p> <p><a href="#">Using Intelligent Updater files to update content on Symantec Endpoint Protection clients</a></p> <p>To update other kinds of content, you must set up and configure a management server to download and to stage the update files.</p> <p><a href="#">Using third-party distribution tools to update client computers</a></p>

---

The following figure shows an example distribution architecture for smaller networks.



The following figure shows an example distribution architecture for larger networks.



[Choose a distribution method to update content on clients based on the platform](#)

[How to update content and definitions on the clients](#)

[Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager](#)

## Choose a distribution method to update content on clients based on the platform

The methods that you can use to distribute virus definitions and other content to the client computers depends on the client platform.

**Table 139: Content distribution method based on Windows, Mac, and Linux clients**

Platform	Method
Windows	<p>By default, the Windows client gets content from the management server.</p> <p>Windows clients can also get updates from the following sources:</p> <ul style="list-style-type: none"><li>• A LiveUpdate server (external or internal) <a href="#">Configuring clients to download content from an internal LiveUpdate server</a> <a href="#">Configuring clients to download content from an external LiveUpdate server</a></li><li>• An external LiveUpdate server (testing only) <a href="#">Testing engine updates before they release on Windows clients</a></li><li>• A Group Update Provider <a href="#">Using Group Update Providers to distribute content to clients</a></li><li>• Third-party distribution tools <a href="#">Distributing the content using third-party distribution tools</a></li><li>• Intelligent Updater <a href="#">Using Intelligent Updater files to update content on Symantec Endpoint Protection clients</a></li></ul> <p><a href="#">Choose a distribution method to update content on clients</a></p> <p>For Windows clients, you can also customize the following settings:</p> <ul style="list-style-type: none"><li>• The content types that the client receives</li><li>• Whether the client can get definitions from multiple sources</li><li>• Whether the client can get smaller packages (deltas) from LiveUpdate if the management server can provide only full definition packages</li></ul> <p>Full definition packages are very large. Too many downloads of full packages can overload your network. Deltas are typically much smaller, and affect your network bandwidth much less.</p> <p><a href="#">Mitigating network overloads for client update requests</a></p>
Mac or Linux	<ul style="list-style-type: none"><li>• A LiveUpdate server (external or internal)</li><li>• An Apache Web server that you configure as a reverse proxy <a href="#">Enabling Mac or Linux clients to download LiveUpdate content using the Apache Web server as a reverse proxy</a></li></ul>

[Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager](#)

[About the types of content that LiveUpdate downloads](#)

[How to update content and definitions on the clients](#)

## Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager

When you configure the management server to download LiveUpdate content, you have to make a number of decisions. When you download content to Symantec Endpoint Protection Manager, you download the content for all the management servers in the site.

### Decisions to make about downloading content



**Table 140: Decisions about content downloads**

Decision	Description
What LiveUpdate server should serve the content to the site?	<p>You can specify either an external Symantec LiveUpdate server (recommended), or one or more internal LiveUpdate servers that have previously been installed and configured.</p> <p>You should not install Symantec Endpoint Protection Manager and an internal LiveUpdate server on the same physical hardware or virtual machine. Installation on the same computer can result in significant server performance problems.</p> <p>If you decide to use one or more internal LiveUpdate servers, you may want to add the Symantec public LiveUpdate server as the last entry. If your clients cannot reach any server on the list, then they are still able to update from the Symantec LiveUpdate server.</p> <p>To continue using an internal LiveUpdate server, you should upgrade to the latest version of LiveUpdate Administrator.</p> <p><a href="#">Downloading LiveUpdate Administrator</a></p> <p><a href="#">Configuring clients to download content from an external LiveUpdate server</a></p> <p><a href="#">Configuring clients to download content from an internal LiveUpdate server</a></p> <p><a href="#">Choose a distribution method to update content on clients</a></p>
How many content revisions should the site store?	<p>The management server stores only the most recent full content package, plus incremental deltas for as many revisions as you specify here. This approach reduces the disk space that is required to store multiple content revisions on the server.</p> <p>The number of clients you select during the Symantec Endpoint Protection Manager installation defines the number of revisions the server stores.</p> <p>For each LiveUpdate content type, the default values are as follows:</p> <ul style="list-style-type: none"> <li>• If you do not check <b>Management server will manage fewer than 500 clients</b>, Symantec Endpoint Protection Manager stores 21 revisions.</li> <li>• If you check <b>Management server will manage fewer than 500 clients</b>, Symantec Endpoint Protection Manager stores 90 revisions.</li> </ul> <p>In most instances during an upgrade, the installation increases the number of revisions to match these new defaults. This increase occurs if the number of revisions you had before the upgrade is less than the new minimum default, based on the above criteria.</p> <p><a href="#">Reverting to an older version of the Symantec Endpoint Protection security updates</a></p>
How often should my site check for LiveUpdate content updates?	The default schedule of having Symantec Endpoint Protection Manager run LiveUpdate every four hours is a best practice.
What operating systems am I downloading content to?	LiveUpdate only downloads the content for the specified operating systems.
What content types should I download to the site and to the clients?	<p>Make sure that the site downloads all content updates that are specified in your client LiveUpdate Content policies.</p> <p><a href="#">About the types of content that LiveUpdate downloads</a></p> <p><a href="#">Reverting to an older version of the Symantec Endpoint Protection security updates</a></p>
What languages should be downloaded for product updates?	This setting applies to product updates only; the content updates are downloaded automatically for all languages.
What content size should be downloaded for definitions?	<p>Standard and embedded/VDI clients use a reduced-size set of definitions (only the latest) that is cloud-enabled. Scans on these clients automatically use the extended definitions set in the cloud.</p> <p>The dark network client downloads the entire set of definitions.</p> <p><b>Warning!</b> Your management server must download the correct content for the client types in your network. If the management server does not download the content that your installed clients require, the clients cannot get updates from the management server.</p>

Decision	Description
Should I test engine updates before they are released?	For large organizations, you should test the new engine updates and definitions before they are rolled out to all client computers. You want to test new engine updates with the minimal amount of disruption and downtime. <a href="#">Testing engine updates before they release on Windows clients</a>

## Downloading content from a LiveUpdate server to the Symantec Endpoint Protection Manager

When you download content to a management server, you download it for all the management servers within the site.

To configure a site to download content

1. In the console, click **Admin > Servers**.
2. Under **Servers**, right-click **Local Site**, and then click **Edit Site Properties**.
3. On the **LiveUpdate** tab, make choices from the following available options.
4. Under **LiveUpdate Source Servers**, click **Edit Source Servers** and then inspect the current LiveUpdate server that is used to update the management server. This server is the Symantec LiveUpdate server by default. Then do one of the following:
  - To use the existing LiveUpdate Source server, click **OK**.
  - To use an internal LiveUpdate server, click **Use a specified internal LiveUpdate server** and then click **Add**.

If you selected **Use a specified internal LiveUpdate server**, in the **Add LiveUpdate Server** dialog box, complete the boxes with the information that identifies the LiveUpdate server, and then click **OK**.

You can add more than one server for failover purposes. If one server goes offline, the other server provides support. You can also add the Symantec public LiveUpdate server as the last server in the list. If you add the public server, use <http://liveupdate.symantecliveupdate.com> as the URL.

### NOTE

If you use a UNC server, then LiveUpdate requires that you use the domain or workgroup as part of the user name.

If the computer is in a domain, use the format `domain_name\user_name`.

If the computer is in a workgroup, use the format `computer_name\user_name`.

In the **LiveUpdate Servers** dialog box, click **OK**.

5. Under **Disk Space Management for Downloads**, type the number of LiveUpdate content revisions to keep.
6. In the **Download Schedule** group box, click **Edit Schedule**, set the options for how often the server should check for updates. Click **OK**.
7. Under **Platforms to Download**, click **Change Platforms** and then inspect the platforms list. Uncheck the platforms that you do not want to download content to.
8. Under **Content Types to Download**, inspect the list of update types that are downloaded.

To add or delete an update type, click **Change Selection**, modify the list, and then click **OK**.

The list should match the list of content types that you include in the LiveUpdate Content policy for your client computers.

- 
- Under **Content to Download for Client Types**, decide whether to download and store content for standard and embedded/VDI clients or dark network clients.

#### **WARNING**

You must download content for the client types in your network. If you do not download the content that your installed clients require, the clients cannot get updates from the management server.

To modify the setting, click **Change Selection**, modify the selection, and then click **OK**.

- Under **Languages to Download**, inspect the list of languages of the update types that are downloaded.

To add or delete a language, click **Change Selection**, modify the list, and then click **OK**.

- Click **OK** to save your selections and close the window.

[How to update content and definitions on the clients](#)

## **Checking that Symantec Endpoint Protection Manager has the latest content**

LiveUpdate downloads definitions and other content to Symantec Endpoint Protection Manager on a schedule. However, you can download content at any time if Symantec Endpoint Protection Manager does not have the latest version. Symantec Endpoint Protection Manager then provides this content to the client computers through the default LiveUpdate policy.

To check that Symantec Endpoint Protection Manager has the latest content

- In the console, click **Home**.
- In the Endpoint Status group box, under **Windows Definitions**, compare the dates for **Latest on Manager** and **Latest from Symantec**.
- If the dates do not match, click **Admin > Servers > Local Site (My Site)**.
- Under **Tasks**, click **Download LiveUpdate content > Download**.

If you are unable to update content on Symantec Endpoint Protection Manager through LiveUpdate, you can download a .jdb file from Symantec Security Response. Symantec Endpoint Protection Manager processes the contents of these files and makes them available for clients to download.

[Download .jdb files to update definitions for Endpoint Protection Manager](#)

### **Checking when content was downloaded from LiveUpdate to Symantec Endpoint Protection Manager**

You can determine the date and time when content was last updated on Symantec Endpoint Protection Manager from LiveUpdate.

To check which content was downloaded from LiveUpdate to Symantec Endpoint Protection Manager

- In the console, click **Admin**.
- On the **Admin** page, under **Tasks**, click **Servers** and select the site.
- Do either one of the following tasks:
  - To check the status of the download, click **Show the LiveUpdate Status**.
  - To check the version of the current content that the Symantec Endpoint Protection Manager is using, click **Show the LiveUpdate Status**.
- Click **Close**.

[Troubleshoot LiveUpdate and definition issues with Endpoint Protection Manager](#)

[Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager](#)

## About the types of content that LiveUpdate downloads

By default, Symantec Endpoint Protection Manager downloads all types of content from the public Symantec LiveUpdate servers. The LiveUpdate Content policy then downloads all types of content from Symantec Endpoint Protection Manager to the Windows and Mac clients.

If you do exclude a content type from the site but you remove the content in a LiveUpdate Content policy, that content is not delivered to the clients. Typically, you should not need to exclude the content that Symantec Endpoint Protection Manager downloads. Do not exclude a type of content unless you are certain that you do not need it.

### [Reverting to an older version of the Symantec Endpoint Protection security updates](#)

LiveUpdate does not download updated policies. Symantec Endpoint Protection Manager updates policies to clients when you assign a new policy to a group or when you edit an existing policy.

**Table 141: The content types that you can download from LiveUpdate to the Symantec Endpoint Protection Manager**

Content type	Description
Client product updates	<p>Includes software improvements and critical fixes against security vulnerabilities to the Windows client. For example, an attacker could bypass a Symantec Endpoint Protection protection feature.</p> <p>LiveUpdate downloads the product updates as a full client installation package between RUx releases. Each package carries the same version number but has an updated build number. For example, the first client installation package might be labeled as 14.3.4555.2000 and the second as 14.3.5228.1000. When this option is enabled, the most recent interim package appears in the following locations in the <b>Version Selection</b> drop-down list:</p> <ul style="list-style-type: none"><li>• AutoUpgrade wizard: On the <b>Admin</b> page &gt; <b>Install Packages</b> page &gt; <b>Client Install Package</b> &gt; <b>Upgrade Clients with Package</b> &gt; <b>Upgrade Settings</b> option &gt; <b>General</b> tab. The AutoUpgrade wizard displays the most recent build only.</li><li>• New package: On the <b>Clients</b> page &gt; <b>Install Packages</b> tab &gt; <b>Add a Client Install Package</b> &gt; <b>General</b> tab. This option does not upgrade client installation packages that are new releases and that have major features in them, such as 14.3 RU2 to 14.3 RU3. You must still upgrade using AutoUpgrade or by manually downloading and installing a full client installation package through the Broadcom <a href="#">Download Management</a> page.</li></ul> <p>To update your Mac and Linux clients, you must use the <b>Web link and email</b> and <b>Save package</b> options in the <b>Client Deployment Wizard</b>.</p> <p>In 14.3 RU1 MP1 and earlier, keep this setting unchecked as this option was not used.</p> <p><a href="#">Upgrading to a new release</a></p> <p><a href="#">Upgrading client software with AutoUpgrade</a></p>
Client patches	<p>Includes the same client software improvements and security fixes as product updates, but the patches are downloaded as an incremental delta file (.dax) instead of the full client installation package.</p> <p>To download the content to the clients, go to the <b>LiveUpdate Settings</b> policy &gt; <b>Additional Settings</b> tab, and check <b>Download client patches</b>. This option lets you update client patches from LiveUpdate, the management server, or a Group Update Provider to the clients.</p> <p>This option was renamed from <b>Client security patches</b> in 14.3 RU2.</p>
Virus and Spyware definitions	<p>Separate virus definition packages are available for the x86 and the x64 platforms. This content type also includes the Auto-Protect portal list as well as Power Eraser definitions.</p>
SONAR heuristic signatures	<p>Protects against zero-day attack threats.</p>
Intrusion Prevention signatures	<p>Protects against network threats and host vulnerabilities. Supports the intrusion prevention and detection engines and Memory Exploit Mitigation.</p>

Content type	Description
Host Integrity content	Includes the templates of predefined requirements that enforce updated patches and security measures on the client computer. LiveUpdate downloads templates for the computers that run Windows operating systems and Mac operating systems. <a href="#">Adding a custom requirement from a template</a>
Submission Control signatures	Controls the flow of submissions to Symantec Security Response.
Reputation Settings	Includes the updates to the reputation data that is used in protection.
Extended File Attributes and Signatures	Used to make updating certificates and Download Insight more data-driven. These data-driven downloads help Symantec update trusted signature lists with definition-style updates.
Endpoint Detection and Response	Updates to the Endpoint Detection and Response (EDR) component, which detects and investigates suspicious activities and issues on hosts and endpoints. EDR provides this forensic information to various product components, including submissions and EDR servers. Added in version 14. <a href="#">Endpoint Detection and Response engine updates for 14 RU1 and newer clients</a>
Common Network Transport Library and Configuration	Definitions that the entire product uses to achieve network transportation and telemetry. These definitions are necessary for reputation queries, as well as for submissions and communication with EDR. Definitions in this category include SEPM STIC and SEPC STIC, for the Symantec Endpoint Protection Manager and Symantec Endpoint Protection client, respectively.
Advanced Machine Learning	Definitions that are used in virus and spyware scans for the clients that use a low-bandwidth policy (added in 14.0.1). Use low-bandwidth mode for standard clients and embedded clients in a network with a slow Internet connection. In low-bandwidth mode, LiveUpdate downloads the definitions once per week or less frequently. To use low-bandwidth mode, you must enroll in the cloud and enable the Low Bandwidth policy. Low-bandwidth mode does not work with dark network clients. If you do not enroll the management server in the cloud console, or you do not intend on using a low-bandwidth policy, disable this option to save some bandwidth and disk space on Symantec Endpoint Protection Manager. <a href="#">Updating clients in low-bandwidth environments</a>
WSS Traffic Redirection	Definitions that the Web Security Services (WSS) Traffic Redirection feature uses. WSS Traffic Redirection uses WSS servers to provide secure proxy settings for your web browsers. (Added in 14.1 MP1.)
SymPlatform definitions	Symantec Endpoint Foundation (SEF) is a framework that delivers future protection technologies as content through LiveUpdate. SEF enables you to download new features to your clients without needing to upgrade them. Includes definitions for URL reputation that runs on 14.3 RU1 or later clients.
Application Control content	Definitions that the Application Control engine uses for the Application Control policy. You should always keep this option enabled. This content runs on version 14.2 and later clients only. For older Windows clients, you must upgrade them to 14.2 first.
Policy Command Handler	Content used by the Policy Command Handler engine.
Endpoint Threat Defense for AD Data	Content used by the Active Directory Defense engine. Added in 14.2 RU1.
Browser Extension	Content for the IPS engine that the client uses to block malicious websites on Google Chrome. Added in 14.3 RU2.

#### [LiveUpdate Administrator content options for Endpoint Protection 14](#)

You cannot disable the following types of content in the LiveUpdate Content policy, including **Extended File Attributes and Signatures**, **Endpoint Detection and Response**, **Common Network Transport Library and Configuration**.

**Table 142: Features and the update content that they need**

When you install an unmanaged client	When you update, you need to download these types of content
Virus and Spyware Protection	<ul style="list-style-type: none"> <li>• Virus and Spyware Definitions</li> <li>• SONAR Definitions When you configure content types for download in Site Properties, these are called SONAR heuristic signatures.</li> <li>• Centralized Reputation Settings When you configure content types for download in Site Properties, this content type is called Reputation Settings.</li> <li>• Revocation Data (downloaded by default, not configurable from Symantec Endpoint Protection Manager)</li> <li>• Symantec Allow List (Symantec Whitelist)</li> <li>• Submission Control signatures</li> <li>• Auto-Protect portal list</li> <li>• Power Eraser definitions</li> <li>• Extended File Attributes and Signatures (as of 14)</li> <li>• Endpoint Detection and Response (as of 14)</li> <li>• Common Network Transport Library and Configuration</li> <li>• Advanced Machine Learning (as of 14.1)</li> </ul>
Virus and Spyware Protection > Download Protection	<ul style="list-style-type: none"> <li>• Virus and Spyware Definitions</li> <li>• SONAR Definitions When you configure content types for download in Site Properties, these are called SONAR heuristic signatures.</li> <li>• Centralized Reputation Settings</li> <li>• Revocation Data</li> <li>• Symantec Allow List (Symantec Whitelist)</li> <li>• Intrusion Prevention signatures When you select this option to download, it includes updates to both the Intrusion Prevention signatures and the Intrusion Prevention engines.</li> <li>• Submission Control signatures</li> <li>• Auto-Protect portal list</li> <li>• Power Eraser definitions</li> <li>• Extended File Attributes and Signatures (as of 14)</li> <li>• Endpoint Detection and Response (as of 14)</li> <li>• Common Network Transport Library and Configuration</li> <li>• Advanced Machine Learning (as of 14.1)</li> </ul>

When you install an unmanaged client	When you update, you need to download these types of content
Virus and Spyware Protection > Outlook Scanner	<ul style="list-style-type: none"> <li>• Virus and Spyware Definitions</li> <li>• SONAR Definitions</li> </ul> <p>When you configure content types for download in Site Properties, these are called SONAR heuristic signatures.</p> <ul style="list-style-type: none"> <li>• Centralized Reputation Settings</li> <li>• Revocation Data</li> <li>• Symantec Allow List (Symantec Whitelist)</li> <li>• Submission Control signatures</li> <li>• Auto-Protect Portal List</li> <li>• Power Eraser Definitions</li> <li>• Extended File Attributes and Signatures</li> <li>• Endpoint Detection and Response (as of 14)</li> <li>• Common Network Transport Library and Configuration</li> <li>• Advanced Machine Learning (as of 14.1)</li> </ul>
Virus and Spyware Protection > Notes Scanner	<ul style="list-style-type: none"> <li>• Virus and Spyware Definitions</li> <li>• SONAR Definitions</li> </ul> <p>When you configure content types for download in Site Properties, these are called SONAR heuristic signatures.</p> <ul style="list-style-type: none"> <li>• Centralized Reputation Settings</li> <li>• Revocation Data</li> <li>• Symantec Allow List (Symantec Whitelist)</li> <li>• Submission Control signatures</li> <li>• Auto-Protect Portal List</li> <li>• Power Eraser Definitions</li> <li>• Extended File Attributes and Signatures</li> <li>• Endpoint Detection and Response (as of 14)</li> <li>• Common Network Transport Library and Configuration</li> <li>• Advanced Machine Learning (as of 14.1)</li> </ul>
Proactive Threat Protection > SONAR	SONAR Definitions Submission Control signatures Extended File Attributes and Signatures Advanced Machine Learning
Proactive Threat Protection > Application Control	Submission Control signatures Extended File Attributes and Signatures Application Control content (as of 14.2)
Network Traffic Redirection policy	WSS Traffic Redirection (as of 14.1 MP1)
Network and Host Exploit Mitigation > Intrusion Prevention	<ul style="list-style-type: none"> <li>• Intrusion Prevention signatures</li> </ul> <p>When you select this option to download, it includes updates to both the intrusion prevention signatures and the Intrusion Prevention engines.</p> <ul style="list-style-type: none"> <li>• Submission Control signatures</li> <li>• Extended File Attributes and Signatures</li> <li>• Browser Extension (as of 14.3 RU2)</li> </ul>
Network and Host Exploit Mitigation > Firewall	Submission Control signatures Extended File Attributes and Signatures
Host Integrity	Host Integrity content Submission Control signatures Extended File Attributes and Signatures

---

[Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager](#)

[How to update content and definitions on the clients](#)

[Choose a distribution method to update content on clients](#)

## Configuring clients to download content from an internal LiveUpdate server

By default, your Windows, Mac, and Linux clients get their updates from the management server.

If you manage a large number of clients, you may want to use Group Update Providers (GUPs) for Windows clients. GUPs reduce the load on the management server and are easier to set up than an internal LiveUpdate server.

[Using Group Update Providers to distribute content to clients](#)

If you don't want to use the default management server or Group Update Providers for client updates, you can:

- Set up an internal LiveUpdate server.
- Use a Symantec LiveUpdate server that is external to your network.

To use an internal LiveUpdate server, you must perform the following tasks:

- Install the internal LiveUpdate server.

For more information about using an internal LiveUpdate server, refer to the *LiveUpdate Administrator's Guide*.

### NOTE

Symantec Endpoint Protection Manager no longer includes legacy support for LiveUpdate Administrator 1.x. To continue using an internal LiveUpdate server, you should upgrade to the latest version of LiveUpdate Administrator. Support for LiveUpdate Administrator 2.x and later is always enabled.

- Use the LiveUpdate Settings policy to configure your clients to use that internal LiveUpdate server.

### NOTE

You can specify proxy settings for the clients that connect to an internal LiveUpdate server for updates. The proxy settings are for updates only. They do not apply to other types of external communication that clients use. You configure the proxy for other types of client external communication separately.

[Specifying a proxy server that clients use to communicate to Symantec LiveUpdate or an internal LiveUpdate server](#)

**To configure Windows clients to use an internal LiveUpdate server:**

1. Under **Policies**, click **LiveUpdate**.
2. On the **LiveUpdate Settings** tab, open the policy that you want to edit.
3. Under **Windows Settings**, click **Server Settings**.
4. In the **Server Settings** pane, check **Use a LiveUpdate server**.
5. Click **Use a specified internal LiveUpdate server**, and then click **Add**.
6. In the **Add LiveUpdate Server** dialog box, type the information that you need to identify and communicate with the server that you want to use.

For the **URL**:

- If you use the HTTP or the HTTPS method, type the URL for the server. For example: Domain name: `http://myliveupdateserver.com`
  - IPv4 address: `http://192.168.133.11:7070/clu-prod`
  - IPv6 address: `http://[fd00:fe32::b008]:7070/clu-prod`
- If you use the FTP method, type the FTP address for the server. For example: `ftp://myliveupdateserver.com`
- If you use the LAN method, type the server UNC path name. For example: `\\myliveupdateserver\LUDepot`



- 
7. If required, type in a user name and password for the server, and then click **OK**.

**NOTE**

If you use a UNC server, then LiveUpdate requires that you use the domain or workgroup in addition to the user name. If the computer is part of a domain, use the format domain\_name\user\_name. If the computer is part of a workgroup, use the format computer\_name\user\_name.

8. Under **LiveUpdate Policy**, click **Schedule** to set up a schedule for updates through LiveUpdate, and then click **OK**.

[Configuring the LiveUpdate download schedule to client computers](#)

9. Optionally click **Advanced Settings**.

Decide whether to keep or change the default user settings, product update settings, and non-standard header settings. Generally, you do not want users to modify update settings. You may, however, want to let users manually launch a LiveUpdate session if you do not support hundreds or thousands of clients.

[Configuring the amount of control that users have over LiveUpdate](#)

10. Click **OK**.

**To configure Mac clients or Linux clients to use an internal LiveUpdate server:**

1. On the **Policies** page, click **LiveUpdate**.
2. On the **LiveUpdate Settings** tab, open the policy.
3. Under **Mac Settings** or **Linux Settings**, click **Server Settings**.
4. Click **Use a specified internal LiveUpdate server**, and then click **Add**.
5. In the **Add LiveUpdate Server** dialog box, type the information that you need to identify and communicate with the server that you want to use.  
For the **URL**:
  - If you use the HTTP or the HTTPS method, type the URL for the server. For example: Domain name: http://myliveupdateserver.com
    - IPv4 address: http://192.168.133.11:7070/clu-prod
    - IPv6 address: http://[fd00:fe32::b008]:7070/clu-prod
  - If you use the FTP method, type the FTP address for the server. For example: ftp://myliveupdateserver.com
  - If you use the LAN method, type the server UNC path name. For example: \\myliveupdateserver\LUDepot
6. If required, type in a user name and password for the server and then click **OK**.
7. If your server uses FTP, click **Advanced Server Settings**, click the FTP mode that the server uses, either **Active** or **Passive**, and then click **OK**.
8. To modify the schedule, click **Schedule**.
9. Click **OK**.

[Randomizing content downloads from a LiveUpdate server](#)

[Configuring Windows client updates to run when client computers are idle](#)

[Choose a distribution method to update content on clients](#)

## Configuring clients to download content from an external LiveUpdate server

By default, Symantec Endpoint Protection Manager provides updates to Windows clients. To help mitigate network overloads for Windows client updates, you should also let clients get updates from a LiveUpdate server. Linux and Mac clients must get updates from a LiveUpdate server, or you can set up the Apache web server as a reverse proxy to download updates from the management server.

[Choose a distribution method to update content on clients](#)

[Enabling Mac and Linux clients to download LiveUpdate content using the Apache Web server as a reverse proxy](#)

---

## NOTE

You may also want to establish communication between a proxy server and Symantec Endpoint Protection Manager so that it can connect with Symantec subscription services. A proxy server can provide an additional level of protection between your site and an external Symantec LiveUpdate server.

[Configuring Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate](#)

To configure clients to download content from an external LiveUpdate server

1. In the console, open a LiveUpdate policy, and click **Edit**
2. Under **Windows Settings**, **Mac Settings**, or **Linux Settings**, click **Server Settings**.
3. Click **Use the default Symantec LiveUpdate server** or specify another LiveUpdate server. If needed, specify your proxy configuration.
4. Click **OK**.

[How to update content and definitions on the clients](#)

## Configuring Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate

You can configure Symantec Endpoint Protection Manager to go through a proxy server to connect to the Internet. A proxy server can add a layer of security because only the proxy server is connected directly to the Internet.

To configure Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate

1. In the console, click **Admin**, and then click **Servers**.
2. Under **Servers**, select the management server to which you want to connect a proxy server.
3. Under **Tasks**, click **Edit the server properties**.
4. On the **Proxy Server** tab, under either **HTTP Proxy Settings** or **FTP Proxy Settings**, for **Proxy usage**, select **Use custom proxy settings**.
5. Type in the proxy settings.

For more information on these settings, click **Help**.

6. Click **OK**.

[Specifying a proxy server that clients use to communicate to Symantec LiveUpdate or an internal LiveUpdate server](#)

## Specifying a proxy server that clients use to communicate to Symantec LiveUpdate or an internal LiveUpdate server

You can specify a proxy server that your clients use to communicate with an internal LiveUpdate server. The proxy settings do not affect any settings for Group Update Providers.

---

## NOTE

You configure proxy settings for other client communications separately.

1. **Option 1:** To specify a proxy server that clients on Windows computers or Linux computers use to communicate to Symantec LiveUpdate or an internal LiveUpdate server, in the console, click **Policies**.
2. Under **Policies**, click **LiveUpdate**, and then click the **LiveUpdate Settings** tab.
3. Right-click the policy that you want and then select **Edit**.
4. Under **Windows Settings** or under **Linux Settings**, click **Server Settings**.
5. Under **LiveUpdate Proxy Configuration**, click **Configure Proxy Options**.
6. Do one of the following:
  - For Windows clients, on the **HTTP or HTTPS** tab, select the desired options. You can also specify proxy settings for FTP.
  - For Linux clients, on the **HTTP** tab, select the desired options.See the online Help for more information about the options.
7. Click **OK** in the dialog box.
8. Click **OK**.
9. **Option 2:** To specify a proxy server that clients on Mac computers use to communicate to Symantec LiveUpdate or an internal LiveUpdate server, in the console, click **Clients > Policies**.
10. Under **Location-independent Policies and Settings**, under **Settings**, click **External Communication Settings**.
11. On the **Proxy Server (Mac)** tab, select the desired options.  
See the online Help for more information about the options.
12. Click **OK**.

[How to update content and definitions on the clients](#)

## Configuring the LiveUpdate download schedule to client computers

The LiveUpdate client schedule settings are defined in the LiveUpdate Settings policy. These settings apply to LiveUpdate sessions that get the latest updates from either a Symantec LiveUpdate server or an internal LiveUpdate server.

[Configuring clients to download content from an external LiveUpdate server](#)

[Configuring clients to download content from an internal LiveUpdate server](#)

To save bandwidth, you can let your clients run scheduled LiveUpdate sessions only if either of the following conditions is met:

- Virus and spyware definitions on a client computer are more than 2 days old.
- A client computer is disconnected from Symantec Endpoint Protection Manager for more than 8 hours.

---

## NOTE

To make sure that any client computers that connect to your network infrequently get the latest updates, let these computers get updates from a Symantec LiveUpdate server. These servers are public, and the client therefore does not depend on a connection to your network to get updates.

1. **Option 1:** To configure the schedule for LiveUpdate downloads to Windows client computers, click **Policies** and then click **LiveUpdate**.
2. On the **LiveUpdate Settings** tab, right-click the policy that you want, and then click **Edit**.
3. Under **Windows Settings**, click **Schedule**.
4. Make sure that **Enable LiveUpdate Scheduling** is checked. This option is enabled by default.
5. Specify the frequency.  
If you select **Daily**, also set the time of day to run. If you select **Weekly**, also set the time of day to run and the day of the week to run.
6. If you select any frequency other than **Continuously**, specify the **Retry Window**.  
The **Retry Window** is the number of hours or days that the client computer tries to run LiveUpdate if the scheduled LiveUpdate fails for some reason.
7. Set any additional options, if required. Symantec recommends that you keep the default values for running LiveUpdate if the definitions are out of date, or if the client has not connected recently to the management server.
8. Click **OK**.

[Randomizing content downloads from a LiveUpdate server](#)

9. **Option 2:** To configure the schedule for LiveUpdate downloads to Mac client computers, click **Policies** and then click **LiveUpdate**.
10. On the **LiveUpdate Settings Policy** tab, right-click the policy that you want, and then click **Edit**.
11. Under **Mac Settings**, click **Schedule**.
12. Specify the frequency.  
If you select **Daily**, also set the time of day to run. If you select **Weekly**, also set the time of day to run and the day of the week to run.
13. Click **OK** when finished.
14. **Option 3:** To configure the schedule for LiveUpdate downloads to Linux client computers, on the **LiveUpdate Settings Policy** tab, right-click the policy that you want, and then click **Edit**.
15. Under **Linux Settings**, click **Schedule**.
16. Check **Enable LiveUpdate Scheduling**. This option is enabled by default.

## NOTE

You should not uncheck this box. If you disable **LiveUpdate Scheduling**, Linux clients do not get the latest updates.

17. Specify the frequency.  
If you select **Daily**, also set the time of day to run. If you select **Weekly**, also set the time of day to run and the day of the week to run.

---

18. If you select any frequency other than **Continuously**, specify the **Retry Window**.

The **Retry Window** is the number of hours or days that the client computer tries to run LiveUpdate if the scheduled LiveUpdate fails.

You can also randomize content downloads.

19. Click **OK**.

[How to update content and definitions on the clients](#)

## Configuring the amount of control that users have over LiveUpdate

You may want to allow users who travel to use an Internet connection to get updates directly from a Symantec LiveUpdate server. You can also allow users to modify the LiveUpdate schedule you set up for content downloads.

### NOTE

If an unmanaged client has a LiveUpdate Settings policy assigned to it when an install package is created, the policy settings always take precedence over a user's changes once the user restarts the computer. To install an unmanaged client that retains a user's changes to LiveUpdate settings after the computer is restarted, install the client from the installation file. Do not use a client install package that has been exported from the Symantec Endpoint Protection Manager.

To configure the amount of control that users have over LiveUpdate

1. In the console, click **Policies**.
2. Under **Policies**, click **LiveUpdate**.
3. On the **LiveUpdate Settings** tab, right-click the policy that you want, and then click **Edit**.
4. Under **Windows Settings**, click **Advanced Settings**.
5. Under **User Settings** pane, check **Allow the user to manually launch LiveUpdate**.
6. Optionally, check **Allow the user to modify the LiveUpdate schedule**.
7. Click **OK**.

[Reverting to an older version of the Symantec Endpoint Protection security updates](#)

[Configuring the LiveUpdate download schedule to client computers](#)

## Mitigating network overloads for client update requests

You must manage your networks for the critical but infrequent situation when too many clients simultaneously request a full set of virus and spyware definitions from the management server or from a Group Update Provider. This situation can occur if the management server encounters an error or runs out of disk space, so that the download and update of the definitions on the client then fails. This situation can also occur if the management server does not download a definitions package and a client then requests this specific delta. In either case, the client then must request a package with a full set of definitions from either the management server or from the Group Update Provider.

To help prevent overloads on your network, the management server provides the following features:

- A notification when the management server receives a specified number of requests for a full set of definitions within a specified period of time.  
You set the conditions for this notification based on what constitutes an overload for your environment. To configure the notification, add a **Network load: requests for virus and spyware full definitions** notification condition.

---

### [Setting up administrator notifications](#)

- The ability to let clients get deltas for virus and spyware definitions from a LiveUpdate server if the management server can provide only a full set. In a LiveUpdate Settings policy, click **Advanced Settings > Download smaller client installation packages from a LiveUpdate server**.
- The ability to block clients from downloading a full set of virus and spyware definitions from the management server. If you receive a notification of a network overload, you can block any further downloads of full packages from the management server. You cannot, however, stop any downloads that are already in progress. Configure this option by clicking **Admin > Servers > server\_name > Edit the server properties > Full Definitions Download > Prevent clients from downloading full definition packages**.

### [Full Definitions Download](#)

## About randomization of simultaneous content downloads

The Symantec Endpoint Protection Manager supports randomization of simultaneous content downloads to your clients from the default management server or a Group Update Provider. It also supports the randomization of the content downloads from a LiveUpdate server to your clients. Randomization reduces peak network traffic and is on by default.

You can enable or disable the randomization function. The default setting is enabled. You can also configure a randomization window. The management server uses the randomization window to stagger the timing of the content downloads. Typically, you should not need to change the default randomization settings.

In some cases, however, you might want to increase the randomization window value. For example, you might run the Symantec Endpoint Protection client on multiple virtual machines on the same physical computer that runs the management server. The higher randomization value improves the performance of the server but delays content updates to the virtual machines.

You also might want to increase the randomization window when you have many physical client computers that connect to a single server that runs the management server. In general, the higher the client-to-server ratio, the higher you might want to set the randomization window. The higher randomization value decreases the peak load on the server but delays content updates to the client computers.

In a scenario where you have very few clients and want rapid content delivery, you can set the randomization window to a lower value. The lower randomization value increases the peak load on the server but provides faster content delivery to the clients.

For downloads from the default management server or a Group Update Provider, you configure the randomization settings in the **Communication Settings** dialog box for the selected group. The settings are not part of the LiveUpdate Settings policy.

For downloads from a LiveUpdate server to your clients, you configure the randomization setting as part of the LiveUpdate Settings policy.

### [Randomizing content downloads from the default management server or a Group Update Provider](#)

### [Randomizing content downloads from a LiveUpdate server](#)

### [Configuring clients to download content from an internal LiveUpdate server](#)

## Randomizing content downloads from the default management server or a Group Update Provider

Your default management server or Group Update Providers might experience reduced performance when multiple client computers attempt to download content from them simultaneously. You can set a randomization window in the communication settings for the group to which the client computers belong. Each client computer attempts to download content at a random time that occurs within that window.

---

## NOTE

The communication settings do not control the randomization settings for the client computers that download content from a LiveUpdate server. You can change the randomization settings for those computers in the LiveUpdate Settings policy.

### [Randomizing content downloads from a LiveUpdate server](#)

To randomize content downloads from the default management server or a Group Update Provider

1. In the console, click **Clients**.
2. Under **Clients**, click the group that you want.
3. On the **Policies** tab, under **Location-independent Policies and Settings**, under **Settings**, click **Communication Settings**.
4. In the **Communication Settings** dialog box, under **Download Randomization**, check **Enable randomization**.
5. Optionally, change the randomization window duration.
6. Click **OK**.

### [About randomization of simultaneous content downloads](#)

### [Configuring clients to download content from an internal LiveUpdate server](#)

## Randomizing content downloads from a LiveUpdate server

Your network might experience traffic congestion when multiple client computers attempt to download content from a LiveUpdate server. You can configure the update schedule to include a randomization window on Windows or Linux clients. Each client computer attempts to download content at a random time that occurs within that window.

## NOTE

The schedule settings in the LiveUpdate Settings policy do not control randomization for the client computers that download content from the default management server or from a Group Update provider. You can change the randomization settings for those computers in the **Communication Settings** dialog box for the group to which they belong.

### [Randomizing content downloads from the default management server or a Group Update Provider](#)

To randomize content downloads from a LiveUpdate server

1. Click **Policies**.
2. Under **Policies**, click **LiveUpdate**.
3. On the **LiveUpdate Settings** tab, right-click the policy that you want to edit, and then click **Edit**.
4. Under **Windows Settings**, **Mac Settings**, or **Linux Settings**, click **Schedule**.
5. Under **Download Randomization Options**, check **Randomize the start time to be + or - (in hours)**.

## NOTE

This setting is in days, if you select **Weekly** updates.

6. Optionally, change the duration for the randomized start time.
7. Click **OK**.

### [About randomization of simultaneous content downloads](#)

### [Configuring clients to download content from an internal LiveUpdate server](#)

---

## Configuring Windows client updates to run when client computers are idle

To ease Windows client computer performance issues, you can configure content downloads to run when client computers are idle. This setting is on by default. Several criteria, such as user, CPU, and disc actions, are used to determine when the computer is idle.

If **Idle Detection** is enabled, once an update is due, the following conditions can delay the session:

- The user is not idle.
- The computer is on battery power.
- The CPU is busy.
- The disk I/O is busy.
- No network connection is present.

After one hour, the blocking set is reduced to CPU busy, Disk I/O busy, or no network connection exists. Once the scheduled update is overdue for two hours, as long as a network connection exists, the scheduled LiveUpdate runs regardless of idle status.

To configure Windows client updates to run when client computers are idle

1. Click **Policies**.
2. Under **Policies**, click **LiveUpdate**.
3. On the **LiveUpdate Settings** tab, right-click the policy that you want to edit, and then click **Edit**.
4. Under **Windows Settings**, click **Schedule**.
5. Check **Delay scheduled LiveUpdate until the computer is idle. Overdue sessions will run unconditionally**.
6. Click **OK**.

[Configuring the LiveUpdate download schedule to client computers](#)

[Configuring Windows client updates to run when definitions are old or the computer has been disconnected](#)

## Configuring Windows client updates to run when definitions are old or the computer has been disconnected

You can ensure that Windows clients update when definitions are old, or the computer has been disconnected from the network for a specified amount of time.

### NOTE

If you check both available options, the client computer must meet both conditions.

To configure Windows client updates when definitions are old or the computers is disconnected from the manager



- 
1. Click **Policies**.
  2. Under **Policies**, click **LiveUpdate**.
  3. On the **LiveUpdate Settings** tab, right-click the policy that you want to edit, and then click **Edit**.
  4. Under **Windows Settings**, click **Schedule**.
  5. Check **LiveUpdate runs only if Virus and Spyware definitions are older than:** and then set the number of hours or days.
  6. Check **LiveUpdate runs only if the client is disconnected from Symantec Endpoint Protection Manager for more than:** and then set the number of minutes or hours.
  7. Click **OK**.

[Configuring the LiveUpdate download schedule to client computers](#)

[Configuring Windows client updates to run when client computers are idle](#)

## Configuring clients to download content from the Symantec Endpoint Protection Manager

The default method for downloading content to clients is by using the management server.

You do not define the schedule for the updates from the management server to the clients. The clients download content from the management server based on the communication mode and heartbeat frequency.

To configure clients to download content from the Symantec Endpoint Protection Manager

1. In the console, open a LiveUpdate policy, and click **Edit**
2. Under **Windows Settings**, click **Server Settings**.
3. Make sure that **Use the default management server** is checked.
4. Click **OK**.

[Updating policies and content on the client using push mode or pull mode](#)

## Testing engine updates before they release on Windows clients

Symantec Endpoint Protection contains several engines that carry out parts of its functionality. These engines are binary files (.dll or .exe) and are delivered with the security definitions. Symantec updates the functionality of these engines to enhance Symantec Endpoint Protection's capabilities and to respond to new threats.

While Symantec updates virus definitions several times a day, the engine content is updated on a quarterly basis. Symantec provides the engine updates using LiveUpdate.

As of version 14.0.1 MP1, Symantec provides a special server lets you download and test the engine content before you roll out the content to your production environment. Symantec releases these updates on the Early Adopter server (EAS). Engine updates are released a few weeks before the engines are available for general release on the public LiveUpdate server.

You download the engine updates using the EAS, try them in a lab environment, and let Symantec know of any conflicts you encounter. This process lets Symantec fix these conflicts ahead of the general release.

Use the following process to test engine updates:

[Step 1: Create a group of test computers to receive content](#)

[Step 2: Configure test computers to receive prereleased content from the Early Adopter server](#)

---

[Step 3: Configuring test and non-test computers to a particular engine version](#)

[Step 4: Set up notifications for new engine releases \(optional\)](#)

[Step 5: Monitor the test computers after engine content is released](#)

### **Step 1: Create a group of test computers to receive content**

The most accurate test of engine compatibility is with the production systems that do real work. Create a permanent testing group by selecting a set of client computers to receive EAS content using the following criteria:

- Identify the various types of critical systems within your environment. These systems may vary from each other by hardware, software, or function. For example, you might identify retail systems such as a gold desktop image, point-of-sale systems, and web servers, among other critical systems to test.
- Use multiple systems of each type as some software conflicts may manifest only intermittently. Choose the production systems that already have the installed software that you normally use and that perform a representative load of work.
- Configure the test client computers that receive the early release content like the production computers that you do not test. Both the clients that you test and do not test should have the same Symantec Endpoint Protection features installed and use the same policies.

If you prefer not to use production computers for testing with the EAS, you may use lab-based systems. In this case, you may want to write the automation that exercises the functions of the systems under test and simulate load.

For customers with a small number of client computers, all you need is one Symantec Endpoint Protection Manager and one Symantec Endpoint Protection for Windows client.

### **Step 2: Configure test computers to receive prereleased content from the Early Adopter server**

For the test group, configure LiveUpdate to download the content from the Symantec Early Adopter server by performing the following steps.

#### **To configure a site to download content from the Symantec Early Adopter LiveUpdate server**

1. In the console, click **Admin > Servers**.
2. Under **Servers**, right-click **Local Site**, and then click **Edit Site Properties**.
3. Under **LiveUpdate Source Servers**, click **Edit Source Servers**.
4. In the **LiveUpdate Servers** dialog box, click **Use the Symantec LiveUpdate server for prereleased content**, and then click **OK > OK**.

#### **To configure the managed clients to use the prerelease Symantec Early Adopter LiveUpdate server**

1. In the console, open a new LiveUpdate Settings policy, and click **Policies > LiveUpdate**.
2. Under **Windows Settings**, click **Server Settings > Use a LiveUpdate server > Use the Symantec LiveUpdate server for prereleased content**.
3. Click **OK**, and assign the policy to the test group.

As long as your LiveUpdate Settings policy gets content from the EAS, the test clients continue to receive the prereleased versions of the content.

#### **NOTE**

For non-test groups, keep the LiveUpdate Settings policy configured to the LiveUpdate server that you normally use. After the engines are available for general release, all client computers receive LiveUpdate content, depending on how you configured your client computers to receive it.

[Configuring clients to download content from an internal LiveUpdate server](#)

[Configuring clients to download content from an external LiveUpdate server](#)

### **Step 3: Configuring test and non-test computers to a particular engine version**

Configure several LiveUpdate Content policies so that:

- 
- The test group receives the latest version of the security definitions and engines. This group downloads all future content revisions with the prerelease engine version in it.
  - The non-test groups receive an existing, safe version of the engine.  
Starting in 14.0.1 MP1, you can also lock on an engine version. With this option, clients continue to receive the latest security definitions that are associated with a particular engine, but not the latest engine version.

#### [Reverting to an older version of the Symantec Endpoint Protection security updates](#)

After you are satisfied that the test group functions normally with the prereleased content, you manually choose the next engine version for these non-test groups.

### **Step 4: Set up notifications for new engine releases (optional)**

To get notifications for planned engine releases that LiveUpdate downloads to the Symantec Endpoint Protection Manager, do one of the following tasks:

- Add a notification for when new content has been downloaded to Symantec Endpoint Protection Manager. Starting in 14.0.1 MP1, notifications for new content include new engine releases as well as security definitions. You receive notifications only if one or more LiveUpdate Content policies that specify a content revision by engine version are locked due to an available engine update.

To view notifications, on the **Home** page, in the **Security Status** pane, click **View Notifications**.

#### **NOTE**

Updates on the EAS are as frequent as on the regular LiveUpdate server. If you feel that you receive these notifications too often, configure the notifications to not appear.

#### [Setting up administrator notifications](#)

- For earlier releases, log on to the Customer Subscription Portal.

#### [How PCS Customers can Sign Up for Alerts and Notifications](#)

### **Step 5: Monitor the test computers after engine content is released**

After Symantec publishes an engine update to the EAS, begin monitoring the computers that you configured to receive this content. Monitor the following items:

- Verify that the test computers run the prerelease version of the engine updates.  
[Verifying which engine and definitions run on the client computers](#)
- Uptime and available resources on the servers and other critical infrastructure using tools such as Microsoft System Center Operations Manager.
- The applications that run on the client computers to ensure that they continue to perform as expected.
- The Symantec Endpoint Protection client status to ensure that it remains connected to the management server and is protected.

#### [Checking whether the client is connected to the management server and is protected](#)

In addition, run the client after you modify the policies or run a scan to ensure that the computer functions as expected.

If you notice any unexpected behavior or suspect a software conflict exists with the engine update, contact Support for assistance. Usually, if Symantec confirms that there is a software conflict before the beginning of the phased rollout, Symantec reschedules the publishing, and works with you to correct the issue. Symantec then republishes an updated engine to EAS.

## **Reverting to an older version of the Symantec Endpoint Protection security updates**

By default, the latest version of content that is downloaded from a LiveUpdate server to the management server is automatically downloaded to Windows clients. The LiveUpdate Content policy specifies the type of content that clients are permitted to check for and install.

However, you may need to download an older version of the content in the following cases:

- 
- The latest set of definitions or engine causes a software conflict on the client computers.
  - You want time to test new engines on control groups before the content releases into production.

#### NOTE

Use this feature very carefully. Unchecking a content type means that the feature is not kept up-to-date on the client. This can potentially put your clients at greater risk.

If you set the content type to **Select a revision** and then convert the Symantec Endpoint Protection client to a cloud-managed client, the content does not update on the client. To avoid this issue, make sure you set the content option to **Use latest available** before you convert the client.

To revert to an older version of the Symantec Endpoint Protection security updates

1. In the console, click **Policies > LiveUpdate**, and open a LiveUpdate Content policy.

2. Under **Windows Settings**, click **Security Definitions**.

You cannot roll back content for Mac clients or Linux clients.

3. To roll back the content to a specific version, click one of the following options:

- **Select a revision > Edit**, and select the revision number.

This option locks the clients to one particular set of security definitions. The clients do not receive any new security definitions.

- **Select an engine version > Edit**, and then select the engine version.

As of 14.0.1 MP1, this option locks the clients to one particular engine, but continues to distribute the latest security definitions that are associated with that engine. Select the engine version if you know the current engine works in your environment, and you need to test a newer engine in a different group before you release it. Or, click **Use latest available** for clients to continually receive the latest engine version and definitions for that content type.

14.0.1 and earlier clients ignore this setting.

4. Click **OK**.

You do not need to restart the client computer for the content to update.

5. After you resolved any troubleshooting issues, under **Windows Settings**, click **Security Definitions > Use latest available** for each content type.

[Testing engine updates before they release on Windows clients](#)

[Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager](#)

## Using Group Update Providers to distribute content to clients

A Group Update Provider (GUP) is a client computer that distributes content updates directly to other clients.

Advantages of the GUPs include:

- They conserve bandwidth and management server resources by offloading processing power to the GUP.
- They deliver updates effectively to clients with limited or slow network connectivity.
- They are easier to set up than an internal LiveUpdate server.

**Table 143: Tasks to use Group Update Providers**

Step	Description
Step 1: Understand the differences between the types of Group Update Providers that you can configure	<p>You can set up single, multiple, or cross-subnet Group Update Providers. The type of Group Update Provider that you set up depends on your network and the clients on that network. The types of Group Update Provider are not mutually exclusive. You can configure one or more types of Group Update Provider per policy.</p> <p><a href="#">About the types of Group Update Providers</a></p> <p><a href="#">About the effects of configuring more than one type of Group Update Provider in your network</a></p>
Step 2: Verify client communication	<p>Before you configure Group Update Providers, verify that the client computers can receive content updates from the server. Resolve any client-server communication problems.</p> <p>You can view client-server activity in the System logs on the <b>Logs</b> tab of the <b>Monitors</b> page.</p> <p><a href="#">Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client</a></p>
Step 3: Configure Group Update Providers in one or more LiveUpdate Settings policies	<p>You configure Group Update Providers in the LiveUpdate Settings policy.</p> <p><a href="#">Configuring clients to download content from Group Update Providers</a></p>
Step 4: Assign the LiveUpdate Settings policy to groups	<p>You assign the LiveUpdate Settings policy to the groups that use the Group Update Providers. You also assign the policy to the group in which the Group Update Provider resides.</p> <p>For a single Group Update Provider, you assign one LiveUpdate Settings policy per group per site. For multiple Group Update Providers and explicit lists of Group Update Providers, you assign one LiveUpdate Settings policy to multiple groups across subnets.</p> <p><a href="#">Assigning a policy to a group or location</a></p>
Step 5: Verify that clients are designated as Group Update Providers	<p>To view the client computers that are designated as Group Update Providers, do one of the following tasks:</p> <ul style="list-style-type: none"><li>Click <b>Clients</b> &gt; <b>Clients</b> tab &gt; right-click the client, and then click <b>Edit Properties</b>. The Group Update Provider field is <b>True</b> or <b>False</b>.</li><li><a href="#">Searching for the clients that act as Group Update Providers</a></li></ul>

## About the types of Group Update Providers

You can configure several types of Group Update Providers in a LiveUpdate Settings policy. The types of Group Update Providers that you use depend on how your network is set up. You can configure one or more types of Group Update Provider per policy; they are not mutually exclusive.

**Table 144: When to use a particular type of Group Update Provider**

Group Update Provider Type	When to use
Single	<p>A single Group Update Provider is a dedicated client computer that provides content for one or more groups of clients. Configuring a single Group Update Provider turns a single client into a Group Update Provider. A single Group Update Provider can be a client computer in any group.</p> <p>Use a single Group Update Provider when you want to use the same Group Update Provider for all your client computers.</p> <p>You use a single LiveUpdate Settings policy to specify a static IP address or host name for a single Group Update Provider. However, if the client that serves as a single Group Update Provider changes location, you must change the IP address in the policy.</p> <p>If you want to use different single Group Update Providers in different groups, you must create a separate LiveUpdate Settings policy for each group.</p>
Multiple	<p>Multiple Group Update Providers use a set of rules, or criteria, to elect themselves to serve groups of clients in their own subnets. All client computers are on the same subnet.</p> <p>You specify the criteria that client computers must meet to qualify as a Group Update Provider. If a client computer meets the criteria, the management server adds the client to a global list of Group Update Providers. The management server then makes the global list available to all the clients in the network. Clients check the list and choose the Group Update Providers that are located in their own subnet.</p> <p>Configuring multiple Group Update Providers turns multiple clients into Group Update Providers.</p> <p><b>Use multiple Group Update Providers for any of the following scenarios:</b></p> <ul style="list-style-type: none"> <li>You have multiple groups and want to use different Group Update Providers for each group. You can use one policy that specifies rules for the election of multiple Group Update Providers. If clients change locations, you do not have to update the LiveUpdate Settings policy. The Symantec Endpoint Protection Manager combines multiple Group Update Providers across sites and domains. It makes the list available to all clients in all groups in your network.</li> <li>Multiple Group Update Providers can function as a failover mechanism. The use of Multiple Group Update Providers ensures a higher probability that at least one Group Update Provider is available in each subnet.</li> </ul>
Explicit list	<p>Use an explicit list of Group Update Providers when you want clients to be able to connect to Group Update Providers that are on subnets other than the client's subnet. Clients that change location can roam to the closest Group Update Provider on the list.</p> <p>An explicit Group Update Providers list does not turn clients into Group Update Providers.</p> <p>When you configure an explicit list, you can specify that the clients with IP addresses that fall on a particular subnet should use a particular Group Update Provider. A client may have multiple IP addresses, and the management server considers all of the client's IP addresses when it matches which Group Update Provider to use. So, the IP address that the policy matches to is not necessarily bound to the interface that the client uses to communicate with the Group Update Provider.</p> <p>For example, suppose that a client has IP address A, which it uses to communicate with the management server and with the Group Update Provider. This same client also has IP address B, which is the one that matches the Explicit Group Update Provider that you have configured in the LiveUpdate Settings policy for this client. The client can choose to use a Group Update Provider based on the address B, even though that is not the address that it uses to communicate with the Group Update Provider.</p>

Configuring single or multiple Group Update Providers in a LiveUpdate Settings policy performs the following functions:

- It specifies which clients with this policy are to act as Group Update Providers.
- It specifies which Group Update Providers the clients with this policy should use for content updates.

Configuring an explicit Group Update Provider list performs only one function:

- It specifies which Group Update Providers the clients with this policy should use for content updates.
- Although it does not turn clients into Group Update Providers, you can still configure and apply a policy that contains only an explicit provider list. However, you must then have a single Group Update Provider or multiple Group Update Providers configured in another policy in the Symantec Endpoint Protection Manager. Or, you can have both types configured in other policies.

---

If a client cannot obtain its update through any of the Group Update Providers, it can then optionally try to update from the Symantec Endpoint Protection Manager.

[About the effects of configuring more than one type of Group Update Provider in your network](#)

[Using Group Update Providers to distribute content to clients](#)

[Configuring clients to download content from Group Update Providers](#)

[Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager](#)

## Configuring clients to download content from Group Update Providers

You use the LiveUpdate Settings policy so that clients get updates from the Group Update Provider only and never from the management server. You can set up single, multiple, or cross-subnet Group Update Providers. The type of Group Update Provider that you set up depends on your network and the clients on that network.

[About the types of Group Update Providers](#)

1. To configure clients to download content from Group Update Providers, in the console, click **Policies**.
2. Under **Policies**, click **LiveUpdate**.
3. On the **LiveUpdate Settings** tab, right-click the policy that you want and then click **Edit**.
4. In the **LiveUpdate Settings Policy** window, click **Server Settings**.
5. Under **Internal or External LiveUpdate Server**, check **Use the default management server**.
6. Under **Group Update Provider**, check **Use a Group Update Provider**.
7. Click **Group Update Provider**.
8. Do one of the following tasks:
  - Follow the steps in [To configure a single Group Update Provider](#).
  - Follow the steps in [To configure multiple Group Update Providers](#).
  - Follow the steps in [To configure an explicit list of Group Update Providers](#).
9. Under **Group Update Provider Settings**, configure the options to control how content is downloaded and stored on the Group Update Provider computer.

Click **Help** for information about content downloads.
10. Click **OK**.
11. To configure a single Group Update Provider, in the **Group Update Provider** dialog box, check **Single Group Update Provider IP address or host name**, and type the IP address or host name of the client computer that acts as the single Group Update Provider.

Click **Help** for information about the IP address or host name.

- 
12. Return to the procedure to configure a Group Update Provider.
  13. To configure multiple Group Update Providers, in the **Group Update Provider** dialog box, check **Multiple Group Update Providers**, and then click **Configure Group Update Provider List**.
  14. In the **Group Update Provider List** dialog box, select the tree node **Group Update Provider**, and then click **Add** to add a rule set.
  15. In the **Specify Group Update Provider Rule Criteria** dialog box, in the **Check** drop-down list, select one of the following options:
    - **Computer IP Address or Host Name**
    - **Registry Keys**
    - **Operating System**
  16. If you selected **Computer IP Address or Host Name** or **Registry Keys**, click **Add**.
  17. Type or select the IP address or host name, Windows registry key, or operating system information.  
Click **Help** for information on configuring rules.
  18. Click **OK** until you return to the **Group Update Provider List** dialog box, where you can optionally add more rule sets.
  19. Click **OK**.
  20. Return to the procedure to configure a Group Update Provider.
  21. To configure an explicit list of Group Update Providers, in the **Group Update Provider** dialog box, check **Explicit Group Update Providers for roaming clients**, and then click **Configure Explicit Group Update Provider List**.
  22. Click **Add**.
  23. In the **Add Explicit Group Update Provider** dialog box, type the client subnet that you want to map these Group Update Providers to.  
Click **Specify Client Subnet Mask** to add multiple client subnets at one time.  
[Add Explicit Group Update Provider](#)
  24. Select the **Type** of mapping you want to set up: based on the IP address, the host name, or the Group Update Provider's network address.  
Type in the necessary settings for the type of mapping you selected.
  25. Click **OK**.

[Choose a distribution method to update content on clients](#)

[Using Group Update Providers to distribute content to clients](#)

## Searching for the clients that act as Group Update Providers

You can verify that clients are available as Group Update Providers. You can view a list of Group Update Providers by searching for them on the **Clients** tab.

### NOTE

You can also check a client's properties. The properties include a field that indicates whether or not the client is a Group Update Provider.

To search for the clients that act as Group Update Providers



- 
1. In the console, click **Clients**.
  2. On the **Clients** tab, in the **View** box, select **Client status**.
  3. In the **Tasks** pane, click **Search clients**.
  4. In the **Find** drop-down list, select **Computers**.
  5. In the **In Group** box, specify the group name.
  6. Under **Search Criteria**, click in the **Search Field** column and select **Group Update Provider**.
  7. Under **Search Criteria**, click in the **Comparison Operator** column and select **=**.
  8. Under **Search Criteria**, click in the **Value** column and select **True**.  
Click **Help** for information on the search criteria.
  9. Click **Search**.

[Using Group Update Providers to distribute content to clients](#)

## About the effects of configuring more than one type of Group Update Provider in your network

When you configure single or multiple Group Update Providers in policies, then Symantec Endpoint Protection Manager constructs a global list of all the providers that have checked in. By default, this file is:

**64-bit operating systems:** C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent\gup\globallist.xml

**32-bit operating systems:** C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent\gup\globallist.xml.

Symantec Endpoint Protection Manager provides this global list to any client that asks for it so that the client can determine which Group Update Provider it should use. Because of this process, clients that have policies with only multiple or explicit Group Update Providers configured can also use single Group Update Providers, if the single provider meets the explicit mapping criterion. This phenomenon can occur because single providers are a part of the global list of providers that the clients get from their Symantec Endpoint Protection Manager.

So, all of the Group Update Providers that are configured in any of the policies on a Symantec Endpoint Protection Manager are potentially available for clients' use. If you apply a policy that contains only an explicit Group Update Provider list to the clients in a group, all of the clients in the group attempt to use the Group Update Providers that are in the Symantec Endpoint Protection Manager global Group Update Provider list that meet the explicit mapping criteria.

### NOTE

A Symantec Endpoint Protection client may have multiple IP addresses. Symantec Endpoint Protection considers all IP addresses when it matches to a Group Update Provider. So, the IP address that the policy matches is not always bound to the interface that the client uses to communicate with the Symantec Endpoint Protection Manager and the Group Update Provider.

If all types of Group Update Providers are configured in the policies on a Symantec Endpoint Protection Manager, then clients try to connect to Group Update Providers in the global list in the following order:

- Providers on the **Multiple Group Update Providers** list, in order
- Providers on the **Explicit Group Update Providers** list, in order
- The Provider that is configured as a **Single Group Update Provider**

You can configure the following types of explicit mapping criteria:

- 
- IP address: Clients in subnet A should use the Group Update Provider that has the IP address `x.x.x.x`.
  - Host name: Clients in subnet A should use the Group Update Provider that has the host name `xxxx`.
  - Subnet network address: Clients in subnet A should use any Group Update Provider that resides on `subnet B`.

Multiple mapping criteria can be used in an explicit Group Update Provider list in a single policy. Symantec recommends that you be very careful how you configure multiple mapping criteria to avoid unintended consequences. For example, you can strand your clients without a means of obtaining updates if you misconfigure an explicit mapping.

Consider a scenario with the following multiple explicit mapping criteria configured in a single policy:

- If a client is in subnet 10.1.2.0, use the Group Update Provider that has IP address 10.2.2.24
- If a client is in subnet 10.1.2.0, use the Group Update Provider that has IP address 10.2.2.25
- If a client is in subnet 10.1.2.0, use the Group Update Provider that has host name `SomeMachine`
- If a client is in subnet 10.1.2.0, use any Group Update Provider on subnet 10.5.12.0
- If a client is in subnet 10.6.1.0, use any Group Update Provider on subnet 10.10.10.0

With this explicit Group Update Provider policy, if a client is in subnet 10.1.2.0, the first four rules apply; the fifth rule does not. If the client is in a subnet for which no mapping is specified, such as 10.15.1.0, then none of the rules apply to that client. That client's policy says to use an explicit Group Update Provider list, but there is no mapping that the client can use based on these rules. If you also disabled that client's ability to download updates from Symantec Endpoint Protection Manager and the Symantec LiveUpdate server, then that client has no usable update method.

[About the types of Group Update Providers](#)

[Configuring clients to download content from Group Update Providers](#)

## Using Intelligent Updater files to update content on Symantec Endpoint Protection clients

Symantec recommends that client computers use LiveUpdate to update content on Symantec Endpoint Protection clients. However, if you do not want to use LiveUpdate or if LiveUpdate is not available, you can use an Intelligent Updater file to update clients. The Intelligent Updater .exe files for Windows are designed to update the clients only. Intelligent Updater files do not contain the information that Symantec Endpoint Protection Manager needs to update its managed clients.

The Intelligent Updater file for Windows is a self-executing file that contains virus and spyware definitions. Additional Intelligent Updater files are available for SONAR definitions, and for intrusion prevention signatures. For Mac and for Linux, you can download virus and spyware definitions.

After you download the file, you can use your preferred distribution method to distribute the updates to your clients.

### NOTE

An Intelligent Updater file does not provide updates for any other type of content. For example, Intelligent Updater does not support the extended file attributes and signatures, the Auto-Protect portal list, Power Eraser definitions, or reduced-size definitions.

1. To download an Intelligent Updater file, using your web browser, go to the following page:  
[https://www.symantec.com/security\\_response/definitions.jsp](https://www.symantec.com/security_response/definitions.jsp)
2. From the drop-down list, select one of the available Symantec Endpoint Protection options.  
The page refreshes to display the content available for that version.

3. In a protection category, next to **Download**, click **Definitions**.
4. Click the appropriate file name for the version of the client you want to update.

#### NOTE

For Linux virus definitions, click the **Unix Platforms** tab.

5. When you are prompted for a location in which to save the file, select a folder on your hard drive.
6. Distribute the file to the client computers using your preferred distribution method.
7. To install the virus definitions and security updates files on a client computer, on the client computer, locate the Intelligent Updater file that was distributed to the client.
8. Do one of the following:
  - For Windows: Double-click the .exe file, and then follow the on-screen instructions.
  - For Mac: Double-click the .zip file, double-click the .pkg file, and then follow the on-screen instructions.
  - For Linux: Verify that the file has executable permissions, verify that uudecode and uncompress are installed, and then run the .sh file with superuser privilege. See the following for more information:  
[How to update a Linux-based computer with Intelligent Updater definitions](#)

[Choose a distribution method to update content on clients](#)

## Using third-party distribution tools to update client computers

Some large enterprises rely on third-party distribution tools like IBM Tivoli or Microsoft SMS to distribute content updates to client computers. Symantec Endpoint Protection supports the use of third-party distribution tools to update the managed and unmanaged clients that run Windows operating systems. Mac and Linux clients can only receive content updates from internal or external LiveUpdate servers.

Before you set up the use of third-party distribution tools, you must have already installed Symantec Endpoint Protection Manager and the client computers that you want to update.

**Table 145: Tasks to set up the use of third-party distribution tools for updates**

Task	Description
Configure Symantec Endpoint Protection Manager to receive content updates.	You can configure the management server either to receive content updates automatically or manually. <a href="#">Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager</a> <a href="#">How to update content and definitions on the clients</a>
Configure the group's LiveUpdate Settings policy to allow third-party content update distribution.	If you want to use third-party distribution tools to update managed clients, you must configure the group's LiveUpdate Settings policy to allow it. <a href="#">Configuring a LiveUpdate Settings policy to allow third-party content distribution to managed clients</a>
Prepare unmanaged clients to receive updates from third-party distribution tools.	If you want to use third-party distribution tools to update unmanaged clients, you must first create a registry key on each unmanaged client. <a href="#">Preparing unmanaged clients to receive updates from third-party distribution tools</a>

Task	Description
Locate, copy, and distribute the content.	<p>Each Symantec Endpoint Protection Manager client group has an index2.dax file that is located on the computer that runs Symantec Endpoint Protection Manager. These files are located by default in subfolders under the SEPM_Install\data\outbox\agent folder. To update clients, you need to use the index2.dax files. The default location for SEPM_Install is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager.</p> <p><a href="#">Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager</a>  <a href="#">Distributing the content using third-party distribution tools</a></p>

## Configuring a LiveUpdate Settings policy to allow third-party content distribution to managed clients

If you want to use third-party distribution tools to update managed clients, you must configure the client group's LiveUpdate Settings policy to allow it. You can choose whether to disable the ability of client users to manually perform LiveUpdate.

When you are finished with this procedure, a folder appears on the group's client computers in the following location (for Vista and later operating systems):

C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox

### To enable third-party content distribution to managed clients with a LiveUpdate policy:

1. In the console, click **Policies**.
2. Under **Policies**, click **LiveUpdate**.
3. On the **LiveUpdate Settings** tab, under **Tasks**, click **Add a LiveUpdate Setting Policy**.
4. In the **LiveUpdate Policy** window, in the **Policy name** and **Description** text boxes, type a name and description.
5. Under **Windows Settings**, click **Server Settings**.
6. Under **Third Party Management**, check **Enable third party content management**.
7. Uncheck all other LiveUpdate source options.
8. Click **OK**.
9. In the **Assign Policy** dialog box, click **Yes**.  
Optionally, you can cancel out of this procedure and assign the policy at a later time.
10. In the **Assign LiveUpdate Policy** dialog box, check one or more groups to which to assign this policy, and then click **Assign**.

[Configuring clients to download content from an internal LiveUpdate server](#)

## Preparing unmanaged clients to receive updates from third-party distribution tools

If you install unmanaged clients from the installation file, you cannot immediately use third-party distribution tools to distribute LiveUpdate content or policy updates to them. As a security measure, by default these client computers do not trust or process the content that third-party distribution tools deliver to them.

To successfully use third-party distribution tools to deliver updates, you must first create a Windows registry key on each of the unmanaged clients. The key lets you use the inbox folder on unmanaged clients to distribute LiveUpdate content and policy updates by using third-party distribution tools.

The inbox folder appears on unmanaged clients in the following location (Vista and later operating systems):

---

C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox

Once you create the registry key, you can use a third-party distribution tool to copy content or policy updates to this folder. The Symantec Endpoint Protection client software then trusts and processes the updates.

To prepare unmanaged clients to receive updates from third-party distribution tools

1. On each client computer, use regedit.exe or another Windows registry editing tool to add one of the following Windows registry keys:
  - On clients on a 64-bit computer, add HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\SPE\TPMState
  - On clients on a 32-bit computer, add HKEY\_LOCAL\_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SPE\TPMState
2. Set the value type of the registry key to DWORD (32-bit) or QWORD (64-bit) and the value to hexadecimal 80 as follows:  
`0x00000080 (128)`
3. Save the registry key, and then exit the registry editing tool.

[Using third-party distribution tools to update client computers](#)

[Distributing the content using third-party distribution tools](#)

## Distributing the content using third-party distribution tools

To use third-party distribution tools to distribute content to client computers, you need to use the index2.dax file. The LiveUpdate-related content in the index2 file includes a set of GUIDs called content monikers and their associated sequence numbers. Each content moniker corresponds to a particular content type. Each sequence number in the index2 file corresponds to a revision of a particular content type. Depending on the protection features that you have installed, you need to determine which of the content types you need.

[About the types of content that LiveUpdate downloads](#)

### NOTE

Content monikers typically change with each major release. At times, they may also change for a minor release. Symantec does not typically change the monikers for Release Updates or Maintenance Patches.

You can see a mapping of the moniker to its content type by opening the ContentInfo.txt file. By default, the ContentInfo.txt file is located in C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Inetpub\content\.

For example, you might see the following entry:

```
{535CB6A4-441F-4e8a-A897-804CD859100E}: SEPC Virus Definitions  
Win32 12.1 RU6 - MicroDefsB.CurDefs - SymAllLanguages
```

Each Symantec Endpoint Protection Manager client group has its own index2 file. The index2 file for each client group is found in a folder for that group. By default, the folders for client groups are found in C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent\. The folder name for a client group corresponds to the group policy serial number. You can find the serial number in the **Group Properties** dialog box or on the **Clients** page **Details** tab. The first four hexadecimal values of each group policy serial number match the first four hexadecimal values of that group's folder.

The index2.dax file that managed clients use is encrypted. To look at the contents of the file, open the index2.xml file that is available in the same folder. The index2.xml file provides a list of the content monikers and their sequence (revision) numbers. For example, you might see the following entry:

```
<File Checksum="D5ED508E8CF7A8A4450B0DBA39BCCB25" DeltaFlag="1"
```

---

```
FullSize="625203112" LastModifiedTime="1425983765211" Moniker=
"{535CB6A4-441F-4e8a-A897-804CD859100E}" Seq="150309034"/>
```

The LiveUpdate Content policy for a group specifies either a particular revision of content or the latest content. The sequence number in the index2 file must match the sequence number that corresponds to the content specification in the group's LiveUpdate Content policy. For example, if the policy is configured to **Use latest available** for all content types, then the sequence number for each type is the latest available content. In this example, the distribution only works if the index2 file calls out the sequence numbers (revisions) that correspond to the latest content revision. The distribution fails if the sequence numbers correspond to any other revisions.

#### NOTE

You must use the Copy command to place files into the client's \inbox folder. Using the Move command does not trigger update processing, and the update fails. If you compress content into a single archive for distribution, you should not unzip it directly into the \inbox folder.

To distribute content to clients with third-party distribution tools

1. On the computer that runs the Symantec Endpoint Protection Manager, create a working folder such as \Work\_Dir.
2. Do one of the following actions:
  - For a managed client, in the console, on the **Clients** tab, right-click the group to update, and then click **Properties**.
  - For an unmanaged client, in the console, on the **Clients** tab, right-click **My Company**, and then click **Properties**.
3. Write down the first four hexadecimal values of the **Policy Serial Number**, such as 7B86.

4. Navigate to the following folder:

SEPM\_Install\data\outbox\agent

Where SEPM\_Install represents the installation folder for Symantec Endpoint Protection Manager. The default installation folder is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager.

5. Locate the folder that contains the first four hexadecimal values that match the **Policy Serial Number**.
6. Open that folder, and then copy the index2.dax file to your working folder.
7. Navigate to the following folder:

SEPM\_Install\inetpub\content

Where SEPM\_Install represents the installation folder for Symantec Endpoint Protection Manager. The default installation folder is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager.

8. Open and read ContentInfo.txt to discover the content that each target moniker folder contains.

The contents of each directory are in the following format: target moniker\sequence number\full.zip|full.

9. Copy the contents of each \target moniker folder to your working folder such as \Work\_Dir.
10. Delete all files and folders from each \target moniker so that only the following folder structure and file remain in your working folder:

\\Work\_Dir\target moniker\latest sequence number\full.zip

Your working folder now contains the folder structure and files to distribute to your clients.

11. Use your third-party distribution tools to distribute the content of your working folder to the \\Symantec Endpoint Protection\inbox\ folder on each of the clients.

The end result must look like the following:

\\Symantec Endpoint Protection\inbox\index2.dax

\\Symantec Endpoint Protection\inbox\target moniker\latest sequence number\full.zip

---

Files that are processed successfully are then deleted. Files that are not processed successfully are moved to a subfolder named Invalid. If you see files in an **Invalid** folder under the **inbox** folder, then you must try again with those files.

[Using third-party distribution tools to update client computers](#)

[Preparing unmanaged clients to receive updates from third-party distribution tools](#)

---

# Monitoring, Reporting, and Enforcing Compliance

---

Learn how to run and read reports and logs, and set up Host Integrity

This section this describes how to:

- Set up Host Integrity to ensures that client computers are protected and compliant with your company's security policies.
- Use logs and reports to monitor the security in your environment.
- Manage notifications.

## Setting up Host Integrity

Use Host Integrity policies to make sure that the client computers in your network meet your organization's security policies.

[Tasks to set up Host Integrity policies](#) lists the steps you need to perform to set up security compliance using Host Integrity policies.

**Table 146: Tasks to set up Host Integrity policies**

Step	Description
Step 1: Add a Host Integrity policy that checks for a requirement on the client computer and enforces a remediation action for non-compliant computers	<p>When you add a new policy, perform the following tasks:</p> <ol style="list-style-type: none"><li>1. Choose which types of requirements you want the client computer to check. Create a separate requirement for each type of software (such as applications, files, and patches). <a href="#">About Host Integrity requirements</a> <a href="#">Adding predefined requirements to a Host Integrity policy</a></li><li>2. Configure the remediation actions for non-compliant client computers. Remediation requires that the client computer installs or requests the client user to install the required software. <a href="#">Setting up remediation for a predefined Host Integrity requirement</a></li><li>3. Set the order in which requirements are checked and the remediation is tried. For example, updates should be completed in a specific order so that all updates are applied before the user has to restart the client computer.</li></ol>
Step 2: Set the options for the Host Integrity check and notifications	<ul style="list-style-type: none"><li>• Configure how often the Host Integrity check runs. <a href="#">Configuring the frequency of Host Integrity check settings</a></li><li>• Configure whether or not users can cancel remediation. <a href="#">Allowing users to delay or cancel Host Integrity remediation</a></li><li>• Set up a notification to appear on the client computer when the Host Integrity check either passes or fails. Use the notification to tell the end user what to do next. For example, the end user may need to allow a new patch to download and install on the client computer. <a href="#">Configuring notifications for Host Integrity checks</a></li></ul>
Step 3: Set up peer-to-peer enforcement	<p>If the client computers being tested for Host Integrity compliance are on the same network as already-compliant client computers, you can set up peer-to-peer enforcement. You primarily use peer-to-peer enforcement for file sharing. <a href="#">Blocking a remote computer by configuring peer-to-peer authentication</a></p>
Step 4: Set up a Quarantine policy for non-compliant and unremediated computers (optional)	<p>If the client computer fails the Host Integrity check and does not perform remediation, you can quarantine the computer using a Quarantine policy. <a href="#">Creating a Quarantine policy for a failed Host Integrity check</a></p>



## How Host Integrity works

Host Integrity ensures that client computers are protected and compliant with your company's security policies. You use Host Integrity policies to define, enforce, and restore the security of clients to secure enterprise networks and data.

**Table 147: Process for enforcing security compliance on the client computer**

Step	Description
Step 1: The client computer runs a Host Integrity check on the client computer.	<p>The management server downloads the Host Integrity policy to the client computers in the assigned group. The client computers run the Host Integrity check, which compares each computer's configuration with the requirements that you add to the Host Integrity policy.</p> <p>The Host Integrity policy checks for the existence for antivirus software, patches, hot fixes, and other security requirements. For example, the policy may check whether the latest patches have been applied to the operating system.</p> <p><a href="#">Setting up Host Integrity</a></p>
Step 2: The Host Integrity check passes or fails	<ul style="list-style-type: none"><li>• If the computer meets all of the policy's requirements, the Host Integrity check passes.</li><li>• If the computer does not meet all of the policy's requirements, the Host Integrity check fails. You can also set up the policy to ignore a failed requirement so that the check passes.</li></ul> <p><a href="#">Allowing the Host Integrity check to pass if a requirement fails</a></p> <p>You can also set up peer-to-peer authentication in the Firewall policy, which can grant or block inbound access to the remote computers that have the client installed.</p> <p><a href="#">Blocking a remote computer by configuring peer-to-peer authentication</a></p>
Step 3: Non-compliant computers remediate a failed Host Integrity check (optional)	<ul style="list-style-type: none"><li>• If the Host Integrity check fails, you can configure the client to remediate. To remediate, the client downloads and installs the missing software. You can configure either the client to remediate or the end user to remediate in a predefined requirement or a custom requirement. Host Integrity then rechecks that the client computer installed the software.</li></ul> <p><a href="#">Setting up remediation for a predefined Host Integrity requirement</a></p> <ul style="list-style-type: none"><li>• If the Host Integrity check that verifies remediation still fails, the client applies a Quarantine policy. You can use a Quarantine policy to apply stricter restrictions to the failed computers.</li></ul> <p><a href="#">Creating a Quarantine policy for a failed Host Integrity check</a></p> <ul style="list-style-type: none"><li>• While the client is in the Quarantine location, the Host Integrity check continues to run and to try to remediate. The frequency of the check and remediation settings are based on how you configure the Host Integrity policy. Once the client is remediated and passes the Host Integrity check, the client moves out of the Quarantine location automatically.</li></ul> <p>In some cases, you may need to remediate the client computer manually.</p>
Step 4: The client continues to monitor compliance	<p>The Host Integrity check actively monitors each client's compliance status. If at any time the client's compliance status changes, so do the privileges of the computer.</p> <ul style="list-style-type: none"><li>• If you change a Host Integrity policy, it is downloaded to the client at the next heartbeat. The client then runs a Host Integrity check.</li><li>• If the client switches to a location with a different Host Integrity policy while a Host Integrity check is in progress, the client stops checking. The stop includes any remediation attempts. The user may see a timeout message if a remediation server connection is not available in the new location. When the check is complete, the client discards the results. Then the client immediately runs a new Host Integrity check based on the new policy for the location.</li></ul> <p>You can view the results of the Host Integrity check in the Compliance log.</p> <p><a href="#">Viewing logs</a></p>

## About Host Integrity requirements

When you create a new Host Integrity policy, decide which type of requirements to add.

Each requirement specifies the following items:

- What conditions to check  
For example, a requirement would check whether the latest set of virus definitions is installed on the client computer.
- What remediation actions the client takes if the client fails to pass the condition's requirements  
For example, the remediation action can include a URL where the client can download and install the missing virus definitions.

[Requirement types for Host Integrity policies](#) lists the types of requirements you can use.

**Table 148: Requirement types for Host Integrity policies**

Type	Description
Predefined requirements	Use a predefined requirement to check that a specific application or file is installed and runs on the client. A predefined requirement checks for the status of any of the following types of applications: antivirus software, antispyware software, a firewall, a patch, or a service pack. For example, a patch requirement checks that the client computers run a specific operating system patch. If the predefined requirement does not have enough detail, add a custom requirement and write a script. <a href="#">Adding predefined requirements to a Host Integrity policy</a>
Custom requirements from templates	Templates are predefined custom requirements that Symantec wrote for commonly performed tasks. For example, the client can check that a password has been changed in the last 42 days. You can also use the templates as a basis for writing a custom requirement script. Template requirements are available through the Host Integrity policy LiveUpdate service. You must first set up LiveUpdate to download the Host Integrity templates to the management server. <a href="#">Adding a custom requirement from a template</a> <a href="#">Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager</a>
Custom requirements	Use a custom requirement if neither a predefined requirement nor the templates provide the kind of check that you need. Custom requirements include the same fields as predefined requirements, but provide more flexibility. For example, you can include an antispyware application that is not included in the predefined list of antispyware applications. You can simplify the management of required applications by including similar applications in one custom requirement. For example, you can include Internet browsers such as Internet Explorer and Mozilla Firefox in one requirement. <a href="#">Writing a customized requirement script</a>

## [Setting up Host Integrity](#)

### **Adding predefined requirements to a Host Integrity policy**

A predefined requirement in a Host Integrity policy checks that the client computer runs any of several types of applications such as: antivirus, antispyware, firewall, and so on.

You determine the particular application, such as specific patches for the Windows 7 operating system. You then specify the path where the client computers should get the patch.

To add predefined requirements to a Host Integrity policy

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity policy** page, click **Requirements > Add**.
3. In the **Add Requirement** dialog box, click the **Select requirement** drop-down list, select a predefined requirement, and then click **OK**.
4. Configure the settings and remediation options for the requirement, and then click **OK**.

#### [Setting up remediation for a predefined Host Integrity requirement](#)

For more information, click **Help**.

- 
5. Click **OK**.
  6. Assign the policy to groups or locations.
  7. Click **OK**.

[Adding a custom requirement from a template](#)

[Writing a customized requirement script](#)

## Setting up remediation for a predefined Host Integrity requirement

If the Host Integrity check on a client shows that a requirement failed, you can configure the policy to restore the necessary files. The client restores files by downloading, installing, or running the required applications to meet the requirement. The client computer can then pass the Host Integrity check.

You set up remediation in the same dialog box in which you add a predefined requirement. You specify both the path from which the client downloads the remediation files and how the remediation process is implemented.

You can also enable users to have some control over when they remediate their computers. For example, a restart may cause users to lose their work, so users may want to delay remediation until the end of the day.

After the download, installation, or execution of a command to restore a requirement, the client always retests the requirement. Also, the client logs the results as `pass` or `fail`.

To set up remediation for a predefined Host Integrity requirement

1. In the console, open a Host Integrity policy, and add a predefined requirement.

[Adding predefined requirements to a Host Integrity policy](#)

2. In the **Add Requirement** dialog box, click **Install the <requirement type> if it has not been installed on the client**.
3. Click **Download the installation package**.
4. In the **Download URL** text box, type the URL from where the installation file gets downloaded to the client computer.

[About specifying the file location and execute command for remediation](#)

5. In the **Execute the command** text box, do one of the following tasks:

- If you want the client user to run the installation, leave the text box blank.
- If you want the installation to run automatically, type `%F%`.

The `%F%` variable represents the last downloaded file. You can use any command that can be run from **Start > Run**. For example, to install a patch for Vista, type the command `%Systemroot%\system32\wusa.exe /quiet /norestart %F%`.

6. Optionally set the options to delay or cancel remediation, and then click **OK**.

[Allowing users to delay or cancel Host Integrity remediation](#)

7. Click **OK**.

[Allowing the Host Integrity check to pass if a requirement fails](#)

## Allowing users to delay or cancel Host Integrity remediation

You can allow the user to delay remediation to a more convenient time. If users must restart their computers after they install the software for a requirement, they may want to wait to restart their computers until later.

If the user delays remediation, any of the following events can happen:

- 
- The client logs the event. The Host Integrity status is shown as failed because the requirement is not met. The user can manually run a new Host Integrity check at any time from the client.
  - The Host Integrity check remediation message window does not appear again until the client runs another Host Integrity check. If the user has chosen to be reminded in five minutes, but the Host Integrity check runs every 30 minutes, the message window does not appear until 30 minutes. To avoid confusion for the user, you may want to synchronize the minimum time setting with the Host Integrity check frequency setting.
  - If the user delays the remediation before the next Host Integrity check, the user selection is overridden.
  - If the user delays a remediation action and the client receives an updated policy, the amount of time available for remediation is reset to the new maximum.

To allow users to delay or cancel Host Integrity remediation

1. In the console, open a Host Integrity policy and add a requirement.

[Adding predefined requirements to a Host Integrity policy](#)

2. In the **Add Requirement** dialog box, set up remediation.

[Setting up remediation for a predefined Host Integrity requirement](#)

3. On the dialog box for the requirement, do one of the following tasks, and then click **OK**:

- To let the client user delay a file from being downloaded, check **Specify wait time before attempting the download again if the download fails**.
- To let the client user cancel remediation, check **Allow the user to cancel the download for Host Integrity remediation**.

4. Click **OK**.

5. Click **Advanced Settings**.

6. On the **Advanced Settings** page, under **Remediation Dialog Options**, configure the options for canceling the remediation.

7. To add a custom message on the client computer, click **Set Additional Text**.

The message you type appears on the client remediation window if the user clicks **Details**.

8. Click **OK**.

## Configuring the frequency of Host Integrity check settings

You can configure how the Host Integrity check is carried out and how the results are handled.

After you add or update a Host Integrity policy, the policy is downloaded to the client at the next heartbeat. The client then runs the Host Integrity check.

If the user switches to a location with a different policy while a Host Integrity check is in progress, the client stops the check. The stop includes remediation attempts, if required by the policy. The user may get a timeout message if a remediation server connection is not available in the new location. When the check is complete, the client discards the results. Then the client immediately runs a new Host Integrity check based on the new policy for the location.

If the policy is the same in the new location, the client maintains any Host Integrity timer settings. The client runs a new Host Integrity check only when required by the policy settings.

To configure the frequency of Host Integrity check settings

- 
1. In the console, open a Host Integrity policy, and click **Advanced Settings**.
  2. On the **Advanced Settings** page, under **Host Integrity Checking Options**, set the Host Integrity check frequency.
  3. Click **OK**.

[Adding predefined requirements to a Host Integrity policy](#)

[Allowing the Host Integrity check to pass if a requirement fails](#)

## Allowing the Host Integrity check to pass if a requirement fails

Users may need to continue working even if their computers fail the Host Integrity check. You can let the Host Integrity check pass even if a specific requirement fails. The client logs the results but ignores the results.

You apply this setting for a specific requirement. If you want to apply this setting to all requirements, you must enable the setting on each requirement separately. The setting is disabled by default.

To allow the Host Integrity check to pass if a requirement fails

1. In the console, open a Host Integrity policy.
2. Add a predefined requirement or a custom requirement, and then click **OK**.

[Adding predefined requirements to a Host Integrity policy](#)

[Writing a customized requirement script](#)

3. On the dialog box for the requirement, check **Allow the Host Integrity check to pass even if this requirement fails**, and then click **OK**.
4. Click **OK**.

## Configuring notifications for Host Integrity checks

When the client runs a Host Integrity check, you can configure notifications to appear when the following conditions occur:

- A Host Integrity check fails.
- A Host Integrity check passes after it previously failed.

The results of the Host Integrity check appear in the client's Security log. They are uploaded to the Compliance log on the **Monitors** page of the management server.

The client's Security log contains several panes. If you select a Host Integrity check event type, the lower left-hand pane lists whether the individual requirement has passed or failed. The lower right-hand pane lists the conditions of the requirement. You can configure the client to suppress the information in the lower right-hand pane. Although you may need this information when troubleshooting, you may not want users to view the information. For example, you may write a custom requirement that specifies a registry value or a file name. The details are still recorded in the Security log.

You can also enable a notification that gives the user the choice to download the software immediately or delay the remediation.

[Allowing users to delay or cancel Host Integrity remediation](#)

To configure notifications for Host Integrity checks

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity** page, click **Advanced Settings**.
3. On the **Advanced Settings** page, under **Notifications**, to show detailed requirement information, check **Show verbose Host Integrity Logging**.

The lower right-hand pane of the client's Security log displays complete information about a Host Integrity requirement.

---

4. Check any of the following options:

- **Display a notification message when a Host Integrity check fails.**
- **Display a notification message when a Host Integrity check passes after previously failing.**

5. To add a custom message, click **Set Additional Text**, type up to 512 characters of additional text, and then click **OK**.

6. When you are finished with the configuration of this policy, click **OK**.

## Creating a Quarantine policy for a failed Host Integrity check

You use a Quarantine policy for the client computers that fail the Host Integrity check, try to remediate, and then fail remediation again. After the client computer fails remediation, it automatically switches to a Quarantine location, where a Quarantine policy is applied to the computer. You use a Quarantine policy to apply stricter restrictions to the failed computers. You can use any type of protection policy for the Quarantine policy. For example, you can apply a Quarantine Firewall policy that blocks a computer's access to the Internet.

While the client computer is in the Quarantine location, you can configure the Host Integrity check to continue to run and try to remediate the computer. You may also need to remediate the computer manually.

To create a Quarantine policy for a failed Host Integrity check

1. In the console, click **Clients**, and then click the **Policies** tab.
2. On the **Policies** tab, next to **Quarantine Policies when Host Integrity Fails**, click **Add a policy**.
3. In the **Add Quarantine Policy** dialog box, choose a policy type and then click **Next**.
4. Choose whether to use an existing policy, create a new policy, or import a policy file, and then click **Next**.
5. Do one of the following tasks:
  - In the **Add Policy** dialog box, choose the policy, and click **OK**.
  - In the **Policy Type** dialog box, configure the policy, and click **OK**.
  - In the **Import Policy** dialog box, locate the `.dat` file and click **Import**.

[Setting up remediation for a predefined Host Integrity requirement](#)

[About Host Integrity requirements](#)

## Blocking a remote computer by configuring peer-to-peer authentication

You can use peer-to-peer authentication to allow a remote client computer (peer) to connect to another client computer (authenticator) within the same corporate network. The authenticator temporarily blocks inbound TCP and UDP traffic from the remote computer until the remote computer passes the Host Integrity check. You can use this enforcement technique when the remote computer is physically remote. The technique leverages advanced capabilities of the Symantec Endpoint Protection firewall to enhance access to shared files.

**The Host Integrity check verifies the following characteristics of the remote computer:**

- The remote computer has Symantec Endpoint Protection installed.
- The remote computer passed the Host Integrity check.

If the remote computer passes the Host Integrity check, the authenticator allows inbound connections from the remote computer.

If the remote computer fails the Host Integrity check, the authenticator continues to block the remote computer. You can specify how long the remote computer is blocked before it can try to connect to the authenticator again. You can also specify certain remote computers to always be allowed, even if they do not pass the Host Integrity check. If you do not enable a Host Integrity policy for the remote computer, the remote computer passes the Host Integrity check.

Peer-to-peer authentication information appears in the Network and Host Exploit Mitigation Traffic log.

---

## NOTE

Peer-to-peer authentication works in server control and mixed control, but not in client control.

To block a remote computer by configuring peer-to-peer authentication

1. In the console, open a Firewall policy.
2. On the **Firewall policy** page, click **Peer-to-Peer Authentication Settings**.
3. On the **Peer-to-Peer Authentication Settings** page, check **Enable peer-to-peer authentication**.
4. Configure each value that is listed on the page.

For more information about these options, click **Help**.

5. To allow remote computers to connect to the client computer without being authenticated, check **Exclude hosts from authentication**, and then click **Excluded Hosts**.

The client computer allows traffic to the computers that are listed in the **Host** list.

6. In the **Excluded Hosts** dialog box, click **Add** to add the remote computers that do not have to be authenticated.
7. In the **Host** dialog box, define the host by IP address, IP range, or the subnet, and then click **OK**.
8. In the **Excluded Hosts** dialog box, click **OK**.
9. Click **OK**.
10. If you are prompted, assign the policy to a group.

[Creating a firewall policy](#)

[Setting up Host Integrity](#)

[Preventing users from disabling protection on client computers](#)

## Adding a custom requirement from a template

Instead of writing custom requirements from scratch, you can add common custom requirements that Symantec created. You use LiveUpdate to download Host Integrity content to the management server. The Host Integrity content includes templates. You then add the custom requirements from the templates to the Host Integrity policy.

To get the latest Host Integrity templates, you must configure a LiveUpdate Content policy to download Host Integrity content.

If you import a requirement a second time and a requirement with the same name exists, the imported requirement does not overwrite the existing requirement. Instead, the imported requirement is shown with the number 2 next to its name on the **Requirements** table.

To add a custom requirement from a template

- 
1. In the console, open a Host Integrity policy.
  2. On the **Host Integrity policy** page, click **Requirements > Add**.
  3. In the **Add Requirement** dialog box, click the **Select requirement** drop-down list, select a predefined requirement, and then click **OK**.
  4. In the **Host Integrity Online Updating** dialog box, expand **Templates**, and then select a template category.
  5. Next to each template you want to add, click **Add**.
  6. Click **Import**.
  7. Click **OK**.

[About Host Integrity requirements](#)

[Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager](#)

[Reverting to an older version of the Symantec Endpoint Protection security updates](#)

## Writing a customized requirement script

Custom requirements provide more flexibility than a predefined requirement. For example, you can add an application that is not included in the predefined lists of applications.

To build a custom requirement, you add one or more functions or **IF..THEN** statements to a script. When you run the script, the Host Integrity check looks for the condition that is listed under the **IF** node. Depending upon the condition, the action that is listed under the **THEN** node is executed. The result (*pass* or *fail*) is returned.

When you add many different conditions in one script to check for, this setting applies to the entire custom requirement script. This choice may affect whether you want to create several small custom requirements or a longer one that includes multiple steps.

To write a customized requirement script

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity policy** page, click **Requirements > Add**.
3. In the **Add Requirement** dialog box, click the **Select requirement** drop-down list, select a predefined requirement, and then click **OK**.
4. In the **Custom Requirement** dialog box, type a name for the requirement.

The requirement name appears on the client computer. The name notifies the user whether the requirement has passed or the requirement has failed or prompts the user to download the software.
5. To add a condition, under **Customized Requirement Script**, click **Add**, and then click **IF..THEN**.

### NOTE

If you first add a function or an **IF..THEN** statement without filling out the fields, an error appears. If you do not want to add the statement, right-click the statement and click **Delete**.

6. With the highlight on the empty condition under the **IF** node, in the right pane, select a condition.

The Host Integrity check looks for the condition on the client computer.
7. Under the **Select a condition** drop-down list, specify the additional information that is required.
8. Under **Customized Requirement Script**, click **THEN**, and then click **Add**.

The **THEN** statement provides the action that should be taken if the condition is true.



---

9. Click any of the following options:

- **IF..THEN**  
Use a nested **IF..THEN** statement to define conditions to check and actions to take if the condition is evaluated as true.
- **Function**  
Use a function to define a remediation action, such as downloading a file.
- **Return**  
Use a return statement to specify whether the results of the evaluation of the condition pass or fail. Every custom requirement must end with a pass or fail statement.
- **Comment** (optional)  
Use a comment to explain the functionality of the conditions, functions, or statements that you add.

10. In the right-hand pane, define the criteria that you added.

For more information on these options, click **Help**.

11. To add more nested statements, conditions, or functions, under **Customized Requirement Script**, right-click the node, and then click **Add**.

12. Repeat steps 9 to 11 as needed.

13. To allow the Host Integrity check to pass no matter what the result, check **Allow the Host Integrity check to pass even if this requirement fails**.

14. Click **OK**.

[Creating a test Host Integrity policy with a custom requirement script](#)

[Adding predefined requirements to a Host Integrity policy](#)

## About registry conditions

You can specify which Windows registry settings to check as part of an **IF..THEN** statement for a customized requirement. You can also specify ways to change registry values. Only `HKEY_CLASSES_ROOT`, `HKEY_CURRENT_USER`, `HKEY_LOCAL_MACHINE`, `HKEY_USERS`, and `HKEY_CURRENT_CONFIG` are supported registry settings.

**When you specify registry keys, remember the following considerations:**

- The key name is limited to 255 characters.
- If the registry key has a backslash (\) at the end, it is interpreted as a registry key. For example: `HKEY_LOCAL_MACHINE\SOFTWARE\`
- If the registry key has no backslash at the end, then it is interpreted as a registry name. For example: `HKEY_LOCAL_MACHINE\SOFTWARE\ActiveTouch`

**When you specify registry values, remember the following considerations:**

- The value name is limited to 255 characters.
- You can check for values as `DWORD` (decimal), `Binary` (hexadecimal), or `String`.
- For `DWORD` values, you can check whether the value is less than, equal to, not equal to, or greater than the specified value.
- For string values, you can check whether the value data equals or contains a given string. If you want the string comparison to be case-sensitive, check the **Match case** check box.
- For binary values, you can check whether the value data equals or contains a given piece of binary data. Hexadecimal bytes represent the data. If you specify value contains, you can also specify the offset for this data. If the offset is left blank, it searches the value for the given binary data. Allowed values for the hexadecimal edit box are 0 through 9 and a through f.

---

The following are examples of registry values:

DWORD	12345 (in decimal)
Binary	31 AF BF 69 74 A3 69 (in hexadecimal)
String	ef4adf4a9d933b747361157b8ce7a22f

## Writing a custom requirement to run a script on the client

In a custom Host Integrity requirement, you can specify a function that causes the client to run a script. You can use a scripting language, such as JScript or VBScript, which you can run with the Microsoft Windows Script Host.

To write a custom requirement to run a script on the client

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity policy** page, click **Requirements > Add**.
3. In the **Add Requirement** dialog box, click the **Select requirement** drop-down list, select a predefined requirement, and then click **OK**.

### Writing a customized requirement script

4. In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.
5. Click **Add**, and then click **Function**.
6. Click **Utility: Run a script**.
7. Enter a file name for the script, such as `myscript.js`.
8. Type the content of the script.
9. In the **Execute the command** text field, type the command to use to execute the script.  
Use `%F` to specify the script file name. The script executes in system context.
10. To specify the amount of time to allow the **Execute** command to complete, select one of the following options:
  - **Do not wait**  
The action returns true if the execution is successful but it does not wait until the execution is completed.
  - **Wait until execution completes**
  - **Enter maximum time**  
Enter a time in seconds. If the `Execute` command does not complete in the specified time, the file execution is terminated.
11. Optionally, uncheck **Delete the temporary file after execution is completed or terminated** if you no longer need it.  
This option is disabled and unavailable if **Do not wait** is selected.
12. Optionally, uncheck **Show new process window** if you do not want to see a window that shows the requirement running the script.

## Writing a custom requirement to set the timestamp of a file

In the custom Host Integrity requirement, you can specify the **Set Timestamp** function to create a Windows registry setting to store the current date and time. You can then use the **Check Timestamp** condition to find out if a specified amount of time has passed since that timestamp was created.

---

For example, if the Host Integrity check runs every 2 minutes, you can specify an action to occur at a longer interval such as a day. In this case, the stored time value is removed. You could set the script to run as follows:

- When the client receives a new profile
  - When the user manually runs a Host Integrity check
1. To write a custom requirement to set the timestamp of a file, in the console, open a Host Integrity policy.
  2. On the **Host Integrity policy** page, click **Requirements > Add**.
  3. In the **Add Requirement** dialog box, click the **Select requirement** drop-down list, select a predefined requirement, and then click **OK**.

#### [Writing a customized requirement script](#)

4. In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.
5. Click **Add**, and then click **Function**.
6. Click **Utility: Set Timestamp**.
7. Type a name up to 255 characters long for the registry setting that stores the date and the time information.  
For example, enter `Date and time of last file update`:
8. To compare the current time to the stored time value, write a custom requirement script.

#### [Writing a customized requirement script](#)

9. In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the condition.
10. Click **Add**, and then click **IF..THEN**.
11. Click **Utility: Check Timestamp**.
12. Type the name you entered for the saved time registry setting.
13. Specify an amount of time in minutes, hours, days, or weeks.

If the specified amount of time has passed, or if the value of the registry setting is empty, the **Set Timestamp** function returns a value of True.

## Writing a custom requirement to increment a registry DWORD value

For a custom requirement, you can increment the Windows registry DWORD value. The **Increment registry DWORD** value function creates the key if it does not exist.

To write a custom requirement to increment the registry DWORD value

1. In the console, add a Host Integrity policy with a custom requirement script.

#### [Writing a customized requirement script](#)

- 
2. In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.
  3. Click **Add**, and then click **Function**.
  4. Click **Registry: Increment registry DWORD value**.
  5. Enter the registry key to check in the **Registry key** field.
  6. Enter a value name to be checked in the **Value name** field.
  7. Click **OK**.

## Creating a test Host Integrity policy with a custom requirement script

The policy that you create for this test is for demonstration purposes only. The policy detects the existence of an operating system and, when detected, generates a `fail` event. Normally, you would generate `fail` events for other reasons.

### Complete the following tasks:

- Add a Host Integrity policy with a custom requirement script that checks for the operating system on the client computer.  
[To create a test Host Integrity policy with a custom requirement script](#)
  - Test the Host Integrity policy you have created.  
[To test the Host Integrity policy on the client computer](#)
1. To create a test Host Integrity policy with a custom requirement script, in the console, open a Host Integrity policy.
  2. On the **Host Integrity policy** page, click **Requirements > Add**.
  3. In the **Add Requirement** dialog box, click the **Select requirement** drop-down list, select a predefined requirement, and then click **OK**.
  4. In the **Name** box, type a name for the custom requirement.
  5. In the **Custom Requirement** dialog box, under **Customized Requirement Script**, right-click **Insert statements below**, and then click **Add > IF..THEN**.
  6. In the right pane, in the **Select a condition** drop-down list, click **Utility: Operating System is**.
  7. Under **Operating system**, check one or more operating systems that your client computers run and that you can test.
  8. Under **Customized Requirement Script**, right-click **THEN //Insert statements here**, and then click **Add > Function > Utility: Show message dialog**.
  9. In the **Caption of the message box** field, type a name to appear in the message title.
  10. In the **Text of the message box** field, type the text that you want the message to display.
  11. In the left pane, under **Customized Requirement Script**, click **Pass**.
  12. In the right pane, under **As the result of the requirement, return**, check **Fail**, and then click **OK**.
  13. Click **OK**.
  14. In the **Host Integrity Policies** dialog box, in the left panel, click **Assign the policy**.
  15. In the **Assign Host Integrity Policy** dialog box, select the groups to which you want to assign the policy, and click **Assign**.

In the **Assign Host Integrity Policy** dialog box, click **Yes** to assign the Host Integrity policy changes.

### NOTE

One Host Integrity policy can be assigned to multiple groups, while a single group can only have a single Host Integrity policy. You can replace an existing policy with a different policy.

- 
16. To test the Host Integrity policy on the client computer, in the console, click **Clients > Clients**.
  17. Under **Clients**, click and highlight the group that contains the client computers to which you applied the Host Integrity policy.
  18. Under **Tasks**, click **Run a command on the group > Update Content**, and then click **OK**.
  19. Log on to the computer that runs the client and note the message box that appears.

Because the rule triggered the `fail` test, the message box appears. After testing, disable or delete the test policy.

[Writing a customized requirement script](#)

[Writing a custom requirement to increment a registry DWORD value](#)

[Writing a custom requirement to run a script on the client](#)

## Monitoring endpoint protection

Symantec Endpoint Protection collects information about the security events in your network. You can use log and reports to view these events, and you can use notifications to stay informed about the events as they occur.

You can use the reports and logs to determine the answers to the following kinds of questions:

- Which computers are infected?
- Which computers need scanning?
- What risks were detected in the network?

**Table 149: Tasks for monitoring endpoint protection**

Task	Description
Review the security status of your network	<p><b>The following list describes some of the tasks that you can perform to monitor the security status of your client computers.</b></p> <ul style="list-style-type: none"> <li>View the number of clients that did not get installed. <a href="#">Running a report on the deployment status of clients</a></li> <li>View the number of computers that are offline. <a href="#">Finding offline computers</a></li> <li>Obtain a count of detected viruses and other security risks and view details for each virus and security risk. <a href="#">Viewing risks</a></li> <li>Obtain a count of unprotected computers in your network and view the details for each computer. <a href="#">Viewing system protection</a></li> <li>View the number of computers with up-to-date virus and spyware definitions. <a href="#">Viewing system protection</a></li> <li>View the real-time operational status of your client computers. <a href="#">Viewing the protection status of client computers</a></li> <li>Review the processes that run in your network. <a href="#">Monitoring SONAR detection results to check for false positives</a></li> <li>Locate which computers are assigned to which groups.</li> <li>View a list of the Symantec Endpoint Protection software versions that are installed on the clients and Symantec Endpoint Protection Manager servers in your network. <a href="#">Generating a list of the Symantec Endpoint Protection versions installed in your network</a></li> <li>View the licensing information on the client computers, which includes the number of valid seats, over-deployed seats, expired seats, and expiration date. <a href="#">Checking the license status in Symantec Endpoint Protection Manager</a></li> </ul> <p><a href="#">Viewing a daily or weekly status report</a> <a href="#">Home page</a></p>
Locate which client computers need protection	<p><b>You can perform the following tasks to view or find which computers need additional protection:</b></p> <ul style="list-style-type: none"> <li>View the number of computers with Symantec Endpoint Protection disabled. <a href="#">Viewing system protection</a></li> <li>View the number of computers with out-of-date virus and spyware definitions. <a href="#">Viewing system protection</a></li> <li>Find the computers that have not been scanned recently. <a href="#">Finding unscanned computers</a></li> <li>View attack targets and sources. <a href="#">Viewing attack targets and sources</a></li> <li>View event logs. <a href="#">Viewing logs</a></li> </ul>
Protect your client computers	<p>You can run commands from the console to protect the client computers. <a href="#">Running commands on client computers from the console</a></p> <p>For example, you can eliminate security risks on client computers. <a href="#">Checking the scan action and rescanning the identified computers</a></p>
Configure notifications to alert you when security events occur	<p>You can create and configure notifications to be triggered when certain security-related events occur. For example, you can set a notification to occur when an intrusion attempt occurs on a client computer. <a href="#">Setting up administrator notifications</a></p>

Task	Description
Create custom quick reports and scheduled reports for ongoing monitoring	<p>You can create and generate customized quick reports and you can schedule custom reports to run regularly with the information that you want to see.</p> <p><a href="#">Running and customizing quick reports</a></p> <p><a href="#">How to run scheduled reports</a></p> <p><a href="#">Saving custom reports</a></p> <p><a href="#">Configuring reporting preferences</a></p>
Minimize the amount of space that client logs take	<p>For security purposes, you might need to retain log records for a longer period of time. However, if you have a large number of clients, you may have a large volume of client log data.</p> <p>If your management server runs low on space, you might need to decrease the log sizes, and the amount of time the database keeps the logs.</p> <p><b>You can reduce the volume of log data by performing the following tasks:</b></p> <ul style="list-style-type: none"> <li>• Upload only some of the client logs to the server, and change the frequency with which the client logs are uploaded. <a href="#">Specifying client log size and which logs to upload to the management server</a></li> <li>• Specify how many log entries the client computer can keep in the database, and how long to keep them. <a href="#">Specifying the log size and how long to keep log entries in the database</a></li> <li>• Filter the less important risk events and system events out so that less data is forwarded to the server. <a href="#">Modifying log handling and notification settings on Windows computers</a></li> <li>• Reduce the number of clients that each management server manages.</li> <li>• Reduce the heartbeat frequency, which controls how often the client logs are uploaded to the server. <a href="#">Updating policies and content on the client using push mode or pull mode</a></li> <li>• Reduce the amount of space in the directory where the log data is stored before being inserted into the database. <a href="#">About increasing the disk space on the server for client log data</a></li> </ul>
Export log data to a centralized location	<p>Log data export is useful if you want to accumulate all logs from your entire network in a centralized location. Log data export is also useful if you want to use a third-party program such as a spreadsheet to organize or manipulate the data. You also might want to export the data in your logs before you delete log records.</p> <p>You can export the data in some logs to a comma-delimited text file. You can export other logs' data to a tab-delimited text file that is called a dump file or to a Syslog server.</p> <p><a href="#">Exporting log data to a text file</a></p> <p><a href="#">Exporting data to a Syslog server</a></p> <p><a href="#">Viewing logs from other sites</a></p>
Troubleshoot issues with reports and logs	<p>You can troubleshoot some issues with reporting.</p> <p><a href="#">Troubleshooting reporting issues</a></p>

## NOTE

Symantec Endpoint Protection pulls the events that appear in the reports from the event logs on your management servers. The event logs contain time-stamps in the client computers' time zones. When the management server receives the events, it converts the event time-stamps to Greenwich Mean Time (GMT) for insertion into the database. When you create reports, the reporting software displays information about events in the local time of the computer on which you view the reports.

## Finding unscanned computers

You can list the computers that need scanning.

### [Monitoring endpoint protection](#)

To find unscanned computers

- 
1. In the console, click **Reports**.
  2. On the **Quick Reports** tab, specify the following information:

Report type	You select <b>Scan</b> .
Selected report	You select <b>Computers Not Scanned</b> .

3. Click **Create Report**.

## Finding offline computers

You can list the computers that are offline.

A client may be offline for a number of reasons. You can identify the computers that are offline and remediate these problems in a number of ways.

[Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)

1. To find offline computers, in the console, click **Home**.
2. On the **Home** page, in the **Endpoint Status** pane, click the link that represents the number of offline computers.
3. To get more information about offline computers, click the **View Details** link.
4. To view offline client computers in the Computer Status log, in the console, click **Monitors**.
5. On the **Logs** tab, from the **Log type** list box, click **Computer Status**.
6. Click **Additional Settings**.
7. In the Online status list box, click **Offline**.
8. Click **View Log**.

By default, a list of the computers that have been offline for the past 24 hours appears. The list includes each computer's name, IP address, and the last time that it checked in with its server. You can adjust the time range to display offline computers for any time range you want to see.

## Generating a list of the Symantec Endpoint Protection versions installed in your network

You can run a quick report from Symantec Endpoint Protection Manager that provides a list of the Symantec Endpoint Protection software versions that are installed in your network. This list can be useful when you want to upgrade or migrate your software from a previous version of Symantec Endpoint Protection. The list includes local and remote computers.

You can save the report using MHTML webpage archive format.



---

### Printing and saving a copy of a report

1. To generate a report that lists the Symantec Endpoint Protection software versions, in the console, click **Reports**.
2. For **Report type**, select **Computer Status**.
3. For **Select a report**, select **Symantec Endpoint Protection Product Versions**.
4. Click **Create Report**.
5. To generate a detailed list of client computers, including Symantec Endpoint Protection software versions, in the console, click **Monitors**, and then click the **Logs** tab.
6. For **Log type**, select **Computer Status**.
7. Adjust the **Time range** if desired, and then click **View log**.
8. Scroll to find the column **Version**. Click on the header to sort by version number.  
Click **View Applied Filters** to adjust the log filters. Click **Export** to export the list. Click a client computer and then click **Details** to see its details.

### Viewing logs

### Choosing which method to upgrade the client software

### Upgrade resources for Symantec Endpoint Protection

## Running a report on the deployment status of clients

You can run several reports on the deployment status of your clients. For example, you can see how many clients were successfully or unsuccessfully installed. You can also see which clients have which protection technologies installed on them, along with system information about the client computers.

### Monitoring endpoint protection

To view the status of deployed clients

1. In the console, click **Reports**.
2. On the **Quick Reports** tab, click the **Computer Status** report type, and then click one of the following reports:
  - For the deployment status of the clients, click **Deployment Report**.
  - For the protection status of the clients, click **Client Inventory Details**.
3. Click **Create Report**.

## Viewing risks

You can get information about the risks in your network.

### Monitoring endpoint protection

1. To view infected and at-risk computers, in the console, click **Reports**.
2. On the **Quick Reports** tab, specify the following information:

Report type	Risk
Selected report	Infected and At Risk Computers

- 
3. Click **Create Report**.
  4. To better understand the benefits and risks of not enabling certain features, you can run the Risk Distribution by Protection Technology report. This report provides the following information:
    - Signature-based detections of virus and spyware
    - SONAR detections
    - Download Insight detections
    - Intrusion Prevention and browser protection detections

To view the risks detected by the types of protection technology, in the console, click **Reports**.

5. On the **Quick Reports** tab, specify the following information:

Report type	<b>Risk</b>
Selected report	<b>Risk Distribution by Protection Technology</b>

6. Click **Create Report**.
7. To view newly detected risks, in the console, click **Reports**.
8. On the **Quick Reports** tab, specify the following information:

Report type	<b>Risk</b>
Selected report	<b>New Risks Detected in the Network</b>

9. Click **Create Report**.
10. To view a comprehensive risk report, in the console, click **Reports**.
11. On the **Quick Reports** tab, specify the following information:

Report type	<b>Risk</b>
Select a report	<b>Comprehensive Risk Report</b>

12. Click **Create Report**.

## Viewing attack targets and sources

You can view attack targets and sources.

### [Monitoring endpoint protection](#)

1. To view the top targets that were attacked, in the console, click **Reports**.
2. On the **Quick Reports** tab, specify the following information:

Report type	You select <b>Network and Host Exploit Mitigation</b> .
Select a report	You select <b>Top Targets Attacked</b> .

3. Click **Create Report**.
4. To view top attack sources, in the console, click **Reports**.
5. On the **Quick Reports** tab, specify the following information:

Report type	You select <b>Network and Host Exploit Mitigation</b> .
Select a report	You select <b>Top Sources of Attack</b> .

- 
- Click **Create Report**.
  - In the console, click **Reports**.
  - On the **Quick Reports** tab, specify the following information:

Report type	You select <b>Network and Host Exploit Mitigation</b> .
Select a report	You select <b>Full Report</b> .
Configure option	You can optionally select the reports to include in the full report.

- Click **Create Report**.

## Viewing a daily or weekly status report

The **Daily Status Report** provides the following information:

- Virus detection counts for cleaned, suspicious, blocked, quarantined, deleted, newly infected, and still infected actions.
- Virus definition distribution timeline
- Top ten risks and infections

The **Weekly Status Report** provides the following information:

- Computer status
- Virus detection
- Protection status snapshot
- Virus definition distribution timeline
- Risk distribution by day
- Top ten risks and infections

### [Monitoring endpoint protection](#)

To view the daily status report

- In the console, click **Home**.
- On the **Home** page, in the **Favorite Reports** pane, click **Symantec Endpoint Protection Daily Status** or **Symantec Endpoint Protection Weekly Status**.

## Viewing system protection

System protection comprises the following information:

- The number of computers with up-to-date virus definitions.
- The number of computers with out-of-date virus definitions.
- The number of computers that are offline.
- The number of computers that are disabled.

### [Monitoring endpoint protection](#)

To view system protection

- In the console, click **Home**.  
System protection is shown in the **Endpoint Status** pane.
- In the **Endpoint Status** pane, click **View Details** to view more system protection information.

## Configuring reporting preferences

You can configure the following reporting preferences:

- 
- The **Home** and **Monitors** pages display options
  - The **Security Status** thresholds
  - The display options that are used for the logs and the reports, as well as legacy log file uploading

The security status thresholds that you set determine when the Security Status message on the Symantec Endpoint Protection Manager **Home** page is considered Poor. Thresholds are expressed as a percentage and reflect when your network is considered to be out of compliance with your security policies.

For example, you can set the percentage of computers with out-of-date virus definitions that triggers a poor security status. You can also set how many days old the definitions need to be to qualify as out of date. Symantec Endpoint Protection determines what is current when it calculates whether signatures or definitions are out of date as follows. Its standard is the most current virus definitions and IPS signature dates that are available on the management server on which the console runs.

For information about the preference options that you can set, you can click **Help** on each tab in the **Preferences** dialog box.

To configure reporting preferences

1. In the console, on the **Home** page, click **Preferences**.
2. Click one of the following tabs, depending on the type of preferences that you want to set:
  - **Home and Monitors**  
[Preferences: Home page and Monitors page](#)
  - **Security Status**  
[Preferences: Security Status](#)
  - **Logs and Reports**  
[Preferences: Logs and Reports](#)
3. Set the values for the options that you want to change.
4. Click **OK**.

## Logging on to reporting from a standalone web browser

You can access the **Home**, **Monitors**, and **Reports** pages from a standalone web browser that is connected to your management server. However, all of the other console functions are not available when you use a standalone browser.

Report pages and log pages always display in the language that the management server was installed with. To display these pages when you use a remote console or browser, you must have the appropriate font installed on the computer that you use.

**To access reporting from a web browser, you must have the following information:**

- The host name of the management server.
- Your user name and password for the management server.

### NOTE

Check the system requirements for the minimum browser version that is supported with the Symantec Endpoint Protection version in use. Earlier web browser versions are not supported.

[Release notes, new fixes, and system requirements for all versions of Endpoint Protection](#)

To log on to reporting from a standalone web browser

1. Open a web browser.
2. Type the default reporting URL into the address text box in the following format:

`https://SEPMServer:8445/reporting`

Where SEPMServer is the host name or IP address of the management server. For a list of supported web browsers, see [Release notes, new fixes, and system requirements for all versions of Endpoint Protection](#).

IP address includes IPv4 and IPv6. You must enclose the IPv6 address with square brackets. For example: `https://[SEPMServer]:8445`

IPv6 is supported as of version 14.2.

#### NOTE

When you enter the HTTPS standalone reporting URL in your browser, the browser might display a warning. The warning appears because the certificate that the management server uses is self-signed. To work around this issue, you can install the certificate in your browser's trusted certificate store. The certificate supports host names only, so use the host name in the URL. If you use localhost, IP address, or the fully qualified domain name, a warning still appears.

3. When the logon dialog box appears, type your user name and password, and then click **Log On**.

If you have more than one domain, in the **Domain** text box, type your domain name.

## About the types of Symantec Endpoint Protection Manager reports

The following categories of reports are available:

- Quick reports, which you run on demand.
- Scheduled reports, which run automatically based on a schedule that you configure.

Reports include the event data that is collected from your management servers as well as from the client computers that communicate with those servers. You can customize reports to provide the information that you want to see.

The quick reports are predefined, but you can customize them and save the filters that you used to create the customized reports. You can use the custom filters to create custom scheduled reports. When you schedule a report to run, you can configure it to be emailed to one or more recipients.

A scheduled report always runs by default. You can change the settings for any scheduled report that has not yet run. You can also delete a single scheduled report or all of the scheduled reports.

**Table 150: Report types available as quick reports and scheduled reports**

Report type	Description
<b>Audit</b>	Displays the information about the policies that clients and locations use currently. It includes information about policy modification activities, such as the event times and types, policy modifications, domains, sites, administrators, and descriptions. <a href="#">Audit log and quick reports</a>
<b>Application and Device Control</b>	Displays the information about events where some type of behavior was blocked. These reports include information about application security alerts, blocked targets, and blocked devices. Blocked targets can be Windows registry keys, DLLs, files, and processes. <a href="#">Application and Device Control logs and quick reports</a>
<b>Compliance</b>	Displays the information about how many clients passed or failed the Host Integrity check.
<b>Computer Status</b>	Displays the information about the operational status of the computers in your network, such as which computers have security features turned off. These reports include information about versions, the clients that have not checked in to the server, client inventory, and online status. <a href="#">Computer Status logs and reports</a>
<b>Deception</b>	Displays the information about Deception activity, such as top computers or users that report Deception activity, and top Deceptors triggered. <a href="#">Deception logs and reports</a>

Report type	Description
<b>Network and Host Exploit Mitigation</b>	Displays the information about intrusion prevention, attacks on the firewall, firewall traffic and packets, and Memory Exploit Mitigation. The Network and Host Exploit Mitigation reports let you track a computer's activity and its interaction with other computers and networks. They record information about the traffic that tries to enter or exit the computers through their network connections. Memory Exploit Mitigation events list which mitigation techniques terminated an application or blocked an exploit from attacking an application. <a href="#">Network and Host Exploit Mitigation logs and quick reports</a>
<b>Risk</b>	Displays the information about risk events on your management servers and their clients. It includes information about SONAR scans. <a href="#">Risk logs and quick reports</a> <a href="#">SONAR logs</a>
<b>Scan</b>	Displays the information about virus and spyware scan activity. <a href="#">Scan logs and quick reports</a>
<b>System</b>	Displays the information about event times, event types, sites, domains, servers, and severity levels. The System reports contain information that is useful for troubleshooting client problems. <a href="#">System logs and quick reports</a>

If you have multiple domains in your network, many reports let you view data for all domains, one site, or a few sites. The default for all quick reports is to show all domains, groups, servers, and so on, as appropriate for the report you select to create.

[Running and customizing quick reports](#)

[How to run scheduled reports](#)

The following section describes the reports by name and their general content. You can configure Basic Settings and Advanced Settings for all reports to refine the data you want to view. You can also save your custom filter with a name to run the same custom report at a later time.

**Table 151: Audit reports**

Report name	Description
<b>Policies Used</b>	This report displays the policies that clients and locations use currently. Information includes the domain name, group name, and the serial number of the policy that is applied to each group.

**Table 152: Application and Device Control reports**

Report name	Description
<b>Top Groups With Most Alerted Application Control Logs</b>	This report consists of a pie chart with the relative bars. It shows the groups with the application control logs that have generated the largest number of security alerts.
<b>Top Targets Blocked</b>	This report consists of a pie chart with the following targets, if applicable: <ul style="list-style-type: none"> <li>• Top Files</li> <li>• Top Registry Keys</li> <li>• Top Processes</li> <li>• Top Modules (dlls)</li> </ul>
<b>Top Devices Blocked</b>	This report consists of a pie chart that shows the devices most frequently blocked from access to your network.

**Table 153: Compliance reports**

Report name	Description
<b>Host Integrity Status</b>	This report displays the clients that have passed or failed the Host Integrity check that runs on their computer.
<b>Clients by Compliance Failure Summary</b>	This report consists a bar chart that shows: <ul style="list-style-type: none"><li>• A count of the unique workstations by the type of control failure event, such as antivirus, firewall, or VPN</li><li>• The total number of clients in the group</li></ul>
<b>Compliance Failure Details</b>	This report consists of a table that displays unique computers by control failure. It shows the criteria and the rule that is involved in each failure, along with the percentage of clients that are deployed and the percentage that failed.
<b>Non-compliant Clients by Location</b>	This report consists of a table that shows the compliance failure events. These events display in groups that are based on their location. Information includes the unique computers that failed, and the percentage of total failures and location failures.

**Table 154: Computer Status reports**

Report name	Description
<b>Virus Definition Distributions</b>	This report displays the unique virus definitions file versions that are used throughout your network and the number of computers and percentage using each version.
<b>Computers Not Recently Updated</b>	This report displays a list of all the computers that have not been recently updated. It also displays the computer's operating system, IP address, user name, and the last time its status was changed.
<b>Symantec Endpoint Protection Product Versions</b>	This report displays the list of version numbers for all the Symantec Endpoint Protection product versions in your network. It also includes the domain and server for each, as well as the number of computers and percentage of each.
<b>Intrusion Prevention Signature Distribution</b>	This report displays the IPS signature file versions that are used throughout your network. It also includes the domain and server for each, as well as the number of computers and percentage of each.
<b>Download Protection Signature Distribution</b>	This report displays the download protection signature file versions that are used throughout your network. It also includes the domain and server for each, as well as the number of computers and percentage of each.
<b>SONAR Signature Distribution</b>	This report displays the SONAR signature file versions that are used throughout your network. It also includes the domain and server for each, as well as the number of computers and percentage of each.
<b>Client Inventory</b>	This report consists of a bar chart that displays the total number of computers and percentages of: <ul style="list-style-type: none"><li>• Operating System</li><li>• Total Memory</li><li>• Free Memory</li><li>• Total Disk Space</li><li>• Free Disk Space</li><li>• Processor Type</li></ul>
<b>Compliance Status Distribution</b>	This report consists of a pie chart with relative bars that show compliance passes and failures by group or by subnet. It shows the number of computers and the percentage of computers that are in compliance.

Report name	Description
<b>Client Online Status</b>	<p>This report consists of pie charts with the relative bars per group or per subnet. It displays the percentage of your computers that are online.</p> <p>Online has the following meanings:</p> <ul style="list-style-type: none"> <li>For the clients that are in push mode, online means that the clients are currently connected to the server</li> <li>For the clients that are in pull mode, online means that the clients have contacted the server within the last two client heartbeats</li> <li>For the clients in remote sites, online means that the clients were online at the time of the last replication</li> </ul>
<b>Clients With Latest Policy</b>	This report consists of pie charts per group or subnet. It displays the number of computers and percentage that have the latest policy applied.
<b>Client Count by Group</b>	This report consists of a table that lists host information by group. It displays the number of clients and users. If you use multiple domains, this information appears by domain.
<b>Security Status Summary</b>	<p>This report reflects the general security status of the network, and displays the number and percentage of computers that have the following status:</p> <ul style="list-style-type: none"> <li>The Antivirus English is off</li> <li>Auto-protect is off</li> <li>Tamper Protection is off</li> <li>Restart is required</li> <li>A Host Integrity check failed</li> <li>Network Threat Protection is off</li> </ul>
<b>Protection Content Versions</b>	<p>This report displays all the proactive protection content versions that are used throughout your network. One pie chart is displayed for each of the following types of protection:</p> <ul style="list-style-type: none"> <li>Decomposer versions</li> <li>Eraser Engine versions</li> <li>SONAR Content versions</li> <li>SONAR Engine versions</li> <li>Commercial Application List versions</li> <li>Content Handler Engine versions</li> <li>Permitted Application List versions</li> <li>The new content types that Symantec Security Response has added</li> </ul>
<b>Symantec Endpoint Protection Licensing Status</b>	This report contains days remaining for trial license expiration and instructions to add new licenses.
<b>Client Inventory Details</b>	This report contains details of client inventory, such as computer specifications and signatures.
<b>Client Software Rollout (Snapshots)</b> Scheduled report only	This report consists of tables that track the progression of client package deployments. The snapshot information lets you see how quickly the rollout progresses, and how many clients are still not fully deployed.
<b>Clients Online/Offline Over Time (Snapshots)</b> Scheduled report only	This report consists of line charts and tables that shows the number of clients online or offline. One chart displays for each of the top targets. The target is either a group or an operating system.
<b>Clients With Latest Policy Over Time (Snapshots)</b> Scheduled report only	This report consists of a line chart that displays the clients that have the latest policy applied. One chart displays for each of the top clients.
<b>Non-Compliant Clients Over Time (Snapshots)</b> Scheduled report only	This report consists of a line chart that shows the percentage of clients that have failed a host integrity check over time. One chart displays for each of the top clients.



Report name	Description
<b>Virus Definition Rollout (Snapshots)</b> Scheduled report only	This report lists the virus definitions package versions that have been rolled out to clients. This information is useful for tracking the progress of deploying new virus definitions from the console.
<b>Deployment Report</b>	This report summarizes the state of client installations and deployments.

**Table 155: Network and Host Exploit Mitigation reports**

Report name	Description
<b>Top Targets Attacked</b>	Includes information such as the number and percentage of attacks, the attack type and severity, and the distribution of attacks. You can view information using groups, subnets, clients, or ports as the target.
<b>Top Sources of Attack</b>	Shows the top hosts that initiated attacks against your network. It includes information such as the number and percentage of attacks, the attack type and severity, and the distribution of attacks.
<b>Top Types of Attack</b>	Includes information such as the number and percentage of events, the group and severity, and the event type and number by group.
<b>Top Blocked Applications</b>	Shows the top applications that were prevented from accessing your network. It includes information such as the number and percentage of attacks, the group and severity, and the event type and number by group.
<b>Attacks Over Time</b>	Shows the attacks during the selected time period. For example, if the time range is the last month, the report displays the total number of attacks per day for the past month. It includes the number and percentage of attacks. You can view attacks for all computers, or by the top operating systems, users, IP addresses, groups, or attack types.
<b>Security Events by Severity</b>	Displays the total number and percentage of security events in your network, ranked according to their severity.
<b>Blocked Applications Over Time</b>	Displays the total number of applications that were prevented from accessing your network over a time period that you select. It includes the event time, the number of attacks, and the percentage. You can display the information for all computers, or by group, IP address, operating system, or user.
<b>Traffic Notifications Over Time</b>	Shows the number of notifications that were based on firewall rule violations over time. The rules that are counted are those where you checked the Send Email Alert option in the Logging column of the Firewall Policy Rules list. You can display the information in this report for all computers, or by group, IP address, operating system, or user.
<b>Top Traffic Notifications</b>	Lists the group or subnet, and the number and percentage of notifications. It shows the number of notifications that were based on firewall rule violations that you configured as important to be notified about. The rules that are counted are those where you checked the Send Email Alert option in the Logging column of the Firewall Policy Rules list. You can view information for all, for the Traffic log, or for the Packet log, grouped by top groups or subnets.
<b>Memory Exploit Mitigation Detections</b>	Displays the number of memory exploit mitigation types that have been blocked or allowed.
<b>Top URL Detections</b>	Lists the URLs that URL reputation blocks.
<b>Full Report</b>	Lists the top Network Threat Protection items in a single report.

**Table 156: Risk reports**

Report name	Description
<b>Infected and At Risk Computers</b>	This report consists of two tables. One table lists computers that have a virus infection, and the other table lists the computers that have a security risk that has not yet been remediated.
<b>Action List</b>	This report consists of a table that shows a count of all the possible actions that were taken when risks were detected. The possible actions are Cleaned, Suspicious, Blocked, Quarantined, Deleted, Pending Repair, Logged Commercial or Forced detections, Newly Infected, and Still Infected. This information also appears on the Symantec Endpoint Protection Home page.
<b>Risk Detections Count</b>	This report consists of a pie chart, a risk table, and an associated relative bar. It shows the number of risk detections by domain, server, or computer. If you have legacy Symantec AntiVirus clients, the report uses the server group rather than the domain.
<b>New Risks Detected in the Network</b>	<p>This report consists of a table and a distribution pie chart. For each new risk, the table provides the following information:</p> <ul style="list-style-type: none"> <li>• Risk name</li> <li>• Risk category or type</li> <li>• First discovered data</li> <li>• First occurrence in the organization</li> <li>• Scan type that first detected it</li> <li>• Domain where it was discovered (server group on legacy computers)</li> <li>• Server where it was discovered (parent server on legacy computers)</li> <li>• Group where it was discovered (parent server on legacy computers)</li> <li>• The computer where it was discovered and the name of the user that was logged on at the time</li> </ul> <p>The pie chart shows new risk distribution by the target selection type: domain (server group on legacy computers), group, server (parent server on legacy computers), computer, or user name.</p>
<b>Top Risk Detection Correlation</b>	<p>This report consists of a three-dimensional bar graph that correlates virus and security risk detections by using two variables. You can select from computer, user name, domain, group, server, or risk name for the x and y axis variables. This report shows the top five instances for each axis variable. If you selected computer as one of the variables and there are fewer than five infected computers, non-infected computers may appear in the graph.</p> <p><b>Note:</b> For computers running legacy versions of Symantec AntiVirus, the server group and parent server are used instead of domain and server.</p>
<b>Download Risk Distribution</b>	This report displays the number of files detected by Download Insight and groups them by sensitivity level. Detailed reports are given to files that have been found. You can also group files by URL, web domain, application, and user-allowed before running the report.
<b>Risk Distribution Summary</b>	This report consists of a pie chart and an associated bar graph that displays a relative percentage for each unique item from the chosen target type. For example, if the chosen target is risk name, the pie chart displays slices for each unique risk. A bar is shown for each risk name and the details include the number of detections and its percentage of the total detections.
<b>Risk Distribution Over Time</b>	This report consists of a table that displays the number of virus and security risk detections per unit of time and a relative bar.
<b>Risk Distribution by Protection Technology</b>	This report displays the number of virus and security risk detections per protection technology.
<b>SONAR Detection Results</b>	<p>This report consists of a pie chart and bar graphs that display the following information:</p> <ul style="list-style-type: none"> <li>• A list of the applications that are labeled as risks that you have added to your exceptions as permitted in your network</li> <li>• A list of the applications that have been detected that are confirmed risks</li> <li>• A list of the applications that have been detected but whose status as a risk is still unconfirmed</li> </ul> <p>For each list, this report displays the company name, the application hash and the version, and the computer involved. For the permitted applications, it also displays the source of the permission.</p>

Report name	Description
<b>SONAR Threat Distribution</b>	Displays the top application names that have been detected with relative bars and a summary table. The detections include applications on the Commercial Applications List and Forced Detections lists. The first summary table contains the application name and the number and percentage of detections.
<b>SONAR Threat Detection Over Time</b>	This report consists of a line chart that displays the number of proactive threat detections for the time period selected. It also contains a table with relative bars that lists the total numbers of the threats that were detected over time.
<b>Action Summary for Top Risks</b>	This report lists the top risks that have been found in your network. For each, it displays action summary bars that show the percentage of each action that was taken when a risk was detected. Actions include quarantined, cleaned, deleted, and so on. This report also shows the percentage of time that each particular action was the first configured action, the second configured action, neither, or unknown.
<b>Number of Notifications</b>	This report consists of a pie chart with an associated relative bar. The charts show the number of notifications that were triggered by the firewall rule violations that you have configured as important to be notified about. It includes the type of notifications and the number of each.
<b>Number of Notifications Over Time</b>	This report consists of a line chart that displays the number of notifications in the network for the time period selected. It also contains a table that lists the number of notifications and percentage over time. You can filter the data to display by the type of notification, acknowledgment status, creator, and notification name.
<b>Weekly Outbreaks</b>	This report displays the number of virus and security risk detections and a relative bar per week for each for the specified time range. A range of one day displays the past week.
<b>Comprehensive Risk Report</b>	This report, by default, includes all of the distribution reports and the new risks report. However, you can configure it to include only certain reports. This report includes the information for all domains.
<b>Symantec Endpoint Protection Daily Status</b>	This report contains virus detection, intervention and definition status for network events over the previous 24 hours.
<b>Symantec Endpoint Protection Weekly Status</b>	This report contains licensing status and virus detection statistics for endpoint computers over the previous week. Data reflects cumulative values unless otherwise noted.

**Table 157: Scan reports**

Report name	Description
<b>Scan Statistics Histogram</b>	<p>This report consists of a histogram where you can select how you want the following information in the scan to be distributed:</p> <ul style="list-style-type: none"> <li>• By the scan time (in seconds)</li> <li>• By the number of risks detected</li> <li>• By the number of files with detections</li> <li>• By the number of files that are scanned</li> <li>• By the number of files that are omitted from scans</li> </ul> <p>You can also configure the bin width and how many bins are used in the histogram. The bin width is the data interval that is used for the group by selection. The number of bins specifies how many times the data interval is repeated in the histogram.</p> <p>The information that displays includes the number of entries and the minimum and the maximum values, as well as the average and the standard deviation.</p> <p>You might want to change the report values to maximize the information that is generated in the report's histogram. For example, you might want to consider the size of your network and the amount of information that you view.</p>
<b>Computers by Last Scan Time</b>	This report shows a list of computers in your security network by the last time scanned. It also includes the IP address and the name of the user that was logged in at the time of the scan.

Report name	Description
<b>Computers Not Scanned</b>	This report shows a list of computers in your security network that have not been scanned and provides the following formation: <ul style="list-style-type: none"> <li>The IP address</li> <li>The time of the last scan</li> <li>The name of the current user or the user that was logged on at the time of the last scan</li> </ul>

**Table 158: System reports**

Report name	Description
<b>Top Clients that Generate Errors</b>	This report consists of a pie chart for each warning condition and error condition. The charts show the relative error count and relative warning count and percentage, by client.
<b>Top Servers that Generate Errors</b>	This report consists of a pie chart for each warning condition and error condition. The chart shows the relative error count and relative warning count and percentage, by server.
<b>Database Replication Failures Over Time</b>	This report consists of a line chart with an associated table that lists the replication failures for the time range selected.
<b>Site Status Report</b>	This report shows a real-time summary of the health status of all sites and information on all servers on the local site.
<b>WSS Integration Token Usage</b>	This report summarizes the usage of the integration token for client authentication with Web and Cloud Access Protection.

## Running and customizing quick reports

Quick reports are predefined, customizable reports. These reports include event data collected from your management servers as well as the client computers that communicate with those servers. Quick reports provide information on events specific to the settings you configure for the report. You can save the report settings so that you can run the same report at a later date, and you can print and save reports.

Quick reports are static; they provide information specific to the time frame you specify for the report. Alternately, you can monitor events in real time using the logs.

- Option 1:** To run a quick report, in the console, click **Reports**.
- On the **Quick Reports** tab, in the **Report type** list box, select the type of report that you want to run.
- In the **Select a report** list box, select the name of the report you want to run.
- Click **Create Report**.
- Option 2:** To customize a quick report, in the console, click **Reports**.
- On the **Quick Reports** tab, in the **Report type** list box, select the type of report that you want to customize.
- In the **Select a report** list box, select the name of the report you want to customize.

For the **Network Compliance Status** report and the **Compliance Status** report, in the **Status** list box, select a saved filter configuration that you want to use, or leave the default filter.

For the **Top Risk Detections Correlation** report, you can select values for the **X-axis** and **Y-axis** list boxes to specify how you want to view the report.

For the **Scan Statistics Histogram Scan** report, you can select values for **Bin width** and **Number of bins**.

For some reports, you can specify how to group the report results in the **Group** list box. For other reports, you can select a target in the **Target** field on which to filter report results.

- 
8. In the **Use a saved filter** list box, select a saved filter configuration that you want to use, or leave the default filter.
  9. Under **What filter settings would you like to use?**, in the **Time range** list box, select the time range for the report.
  10. If you select **Set specific dates**, then use the **Start date** and **End date** list boxes. These options set the time interval that you want to view information about.

When you generate a Computer Status report and select **Set specific dates**, you specify that you want to see all entries that involve a computer that has not checked in with its server since the time you specify in the date and time fields.

11. If you want to configure additional settings for the report, click **Additional Settings** and set the options that you want. You can click **Tell me more** to see descriptions of the filter options in the context-sensitive help.

#### NOTE

The filter option text boxes that accept wildcard characters and search for matches are not case-sensitive. The ASCII asterisk character is the only asterisk character that can be used as a wildcard character.

You can save the report configuration settings if you think you will want to run this report again in the future.

12. Click **Create Report**.

[Saving custom reports](#)

[Printing and saving a copy of a report](#)

[How to run scheduled reports](#)

## Saving custom reports

You can save custom report settings in a filter so that you can generate the report again at a later date. When you save your settings, they are saved in the database. The name that you give to the filter appears in the **Use a saved filter** list box for that type of logs and reports.

#### NOTE

The filter configuration settings that you save are available for your user logon account only. Other users with reporting privileges do not have access to your saved settings.

[Editing the filter used for a scheduled report](#)

You can delete any report configuration that you create. When you delete a configuration, the report is no longer available. The default report configuration name appears in the **Use a saved report** list box and the screen is repopulated with the default configuration settings.

#### NOTE

If you delete an administrator from the management server, you have the option to save the reports that were created by the deleted administrator. The ownership of the reports is changed, and the report names are changed. The new report name is in the format "OriginalName('AdminName') ". For example, a report that was created by administrator JSmith, named `Monday_risk_reports`, would be renamed `Monday_risk_reports(JSmith)`.

[About administrator accounts and access rights](#)

To save a custom report

- 
1. In the console, click **Reports**.
  2. On the **Quick Reports** tab, select a report type from the list box.
  3. Change any basic settings or additional settings for the report.  
In 12.1.x, **Additional Settings** is **Advanced Settings**.
  4. Click **Save Filter**.
  5. In the **Filter name** text box, type a descriptive name for this report filter. Only the first 32 characters of the name that you give display when the filter is added to the **Use a saved filter** list.
  6. Click **OK**.
  7. When the confirmation dialog box appears, click **OK**.

After you save a filter, it appears in the **Use a saved filter** list box for related reports and logs.

## How to run scheduled reports

Scheduled reports are the reports that run automatically based on the schedule that you configure. Scheduled reports are emailed to recipients, so you must include the email address of at least one recipient. After a report runs, the report is emailed to the recipients that you configure as an .mht file attachment.

The data that appears in the scheduled reports is updated in the database every hour. At the time that the management server emails a scheduled report, the data in the report is current to within one hour.

The other reports that contain data over time are updated in the database based on the upload interval that you configured for the client logs.

### [Specifying client log size and which logs to upload to the management server](#)

#### **NOTE**

If you have multiple servers within a site that share a database, only the first-installed server runs the reports scheduled for the site. This default ensures that all the servers in the site do not run the same scheduled scans simultaneously. If you want to designate a different server to run scheduled reports, you can configure this option in the local site properties.

To run scheduled reports

1. In the console, click **Reports**.
2. On the **Scheduled Reports** tab, click **Add**.
3. In the **Report name** text box, type a descriptive name and optionally, type a longer description.

Although you can paste more than 255 characters into the description text box, only 255 characters are saved in the description.

- 
4. If you do not want this report to run until another time, uncheck the **Enable this scheduled report** check box.
  5. Select the report type that you want to schedule from the list box.
  6. Select the name of the specific report that you want to schedule from the list box.
  7. Select the name of the saved filter that you want to use from the list box.
  8. In the **Run every** text box, select the time interval at which you want the report to be emailed to recipients (hours, days, weeks, months). Then, type the value for the time interval you selected. For example, if you want the report to be sent to you every other day, select days and then type 2.
  9. In the **Start after** text box, type the date that you want the report to start or click the calendar icon and select the date. Then, select the hour and minute from the list boxes.
  10. Under **Report Recipients**, type one or more comma-separated email addresses.  
You must already have set up mail server properties for email notifications to work.
  11. Click **OK**.

## Editing the filter used for a scheduled report

You can change the settings for any report that you have already scheduled. The next time the report runs it uses the new filter settings. You can also create additional scheduled reports, which you can base on a previously saved report filter.

Filter storage is based in part on the creator, so problems do not occur when two different users create a filter with the same name. However, an individual user or two users who log on to the default admin account should not create filters with the same name.

### If users create filters with the same name, a conflict can occur under two conditions:

- Two users are logged on to the default admin account on different sites and each creates a filter with the same name.
- One user creates a filter, logs on to a different site, and immediately creates a filter with the same name.

If either condition occurs before site replication takes place, the user subsequently sees two filters with the same name in the filter list. Only one of the filters is usable. If this problem occurs, it is a best practice to delete the usable filter and recreate it with a different name. When you delete the usable filter, you also delete the unusable filter.

### [Saving custom reports](#)

#### NOTE

When you associate a saved filter with a scheduled report, make sure that the filter does not contain custom dates. If the filter specifies a custom date, you get the same report every time the report runs.

### [How to run scheduled reports](#)

To edit the filter used for a scheduled report

1. In the console, click **Reports**.
2. Click **Scheduled Reports**.
3. In the list of reports, click the scheduled report that you want to edit.
4. Click **Edit Filter**.
5. Make the filter changes that you want.
6. Click **Save Filter**.

If you want to retain the original report filter, give this edited filter a new name.

- 
7. Click **OK**.
  8. When the confirmation dialog box appears, click **OK**.

## Printing and saving a copy of a report

You can print a report or save a copy of a Quick Report. You cannot print scheduled reports. A saved file or printed report provides a snapshot of the current data in your reporting database so that you can retain a historical record.

### NOTE

By default, Internet Explorer does not print background colors and images. If this printing option is disabled, the printed report may look different from the report that you created. You can change the settings in your browser to print background colors and images.

### Running and customizing quick reports

When you save a report, you save a snapshot of your security environment that is based on the current data in your reporting database. If you run the same report later, based on the same filter configuration, the new report shows different data.

1. To print a copy of a report, in the report window, click **Print**.
2. In the **Print** dialog box, select the printer you want, if necessary, and then click **Print**.
3. To save a copy of a report, in the report window, click **Save**.
4. In the **File Download** dialog box, click **Save**.
5. In the **Save As** dialog box, in the **Save in selection** dialog box, browse to the location where you want to save the file.
6. In the **File name** list box, change the default file name, if desired.
7. Click **Save**.

The report is saved in MHTML Web page archive format in the location you selected.

8. In the **Download complete** dialog box, click **Close**.

## Viewing logs

You can generate a list of events to view from your logs that are based on a collection of filter settings that you select.

### NOTE

If database errors occur when you view the logs that include a large amount of data, you might want to change the database timeout parameters.

If you get CGI or terminated process errors, you might want to change other timeout parameters.

### Changing timeout parameters for reviewing reports and logs

Reports and logs always appear in the language that the management server was installed with. To display these when you use a remote Symantec Endpoint Protection Manager console or browser, you must have the appropriate font installed on the computer that you use.

### About the types of Symantec Endpoint Protection Manager logs

### Saving and deleting custom logs by using filters

To view a log



- 
1. In the console, click **Monitors**.
  2. On the **Logs** tab, from the **Log type** list box, select the type of log that you want to view.
  3. For some types of logs, a **Log content** list box appears. If it appears, select the log content that you want to view.
  4. In the **Use a saved filter** list box, select a saved filter or leave the value **Default**.
  5. Select a time from the **Time range** list box or leave the default value. If you select **Set specific dates**, then set the date or dates and time from which you want to display entries.
  6. Click **Additional Settings** to limit the number of entries you display.

You can also set any other available **Additional Settings** for the type of log that you selected.

In 12.1.x, **Additional Settings** is **Advanced Settings**.

#### NOTE

The filter option fields that accept wildcard characters and search for matches are not case-sensitive. The ASCII asterisk character is the only asterisk character that can be used as a wildcard character.

7. Click **View Log**.

You can also click **Save Filter** to save the filter configuration to generate the same log view at a later date.

## About the types of Symantec Endpoint Protection Manager logs

Logs contain records about client configuration changes, security-related activities, and errors. These records are called events. The logs display these events with any relevant additional information. Security-related activities include information about virus detections, computer status, and the traffic that enters or exits the client computer.

Logs are an important method for tracking each client computer's activity and its interaction with other computers and networks. You can use this data to analyze the overall security status of the network and modify the protection on the client computers. You can track the trends that relate to viruses, security risks, and attacks. If several people use the same computer, you might be able to identify who introduces risks, and help that person to use better precautions.

You can view the log data on the **Logs** tab of the **Monitors** page.

The management server regularly uploads the information in the logs from the clients to the management server. You can view this information in the logs or in reports. Because reports are static and do not include as much detail as the logs, you might prefer to monitor the network by using logs.

In addition to using the logs to monitor your network, you can take the following actions from various logs:

- Run commands on client computers.  
[Running commands on client computers from the console](#)
- Add several kinds of exceptions.  
[Creating exceptions from log events](#)
- Delete files from the **Quarantine**.  
[Managing quarantined files on your computer](#)

[Log types](#) describes the different types of content that you can view and the actions that you can take from each log.

**Table 159: Log types**

Log type	Contents and actions
<b>Audit</b>	<p>The Audit log contains information about policy modification activity. Available information includes the event time and type; the policy modified; the domain, site, and user name involved; and a description. No actions are associated with this log.</p> <p><a href="#">Audit log and quick reports</a></p>
<b>Application and Device Control</b>	<p>The Application Control log and the Device Control log contain information about events where some type of behavior was blocked.</p> <p><b>The following Application and Device Control logs are available:</b></p> <ul style="list-style-type: none"> <li>• Application Control, which includes information about Tamper Protection</li> <li>• Device Control</li> </ul> <p>Available information includes the time the event occurred, the action taken, and the domain and computer that were involved. It also includes the user that was involved, the severity, the rule that was involved, the caller process, and the target.</p> <p>You can create an application control or Tamper Protection exception from the Application Control log.</p> <p><a href="#">Specifying how Symantec Endpoint Protection handles monitored applications on Windows clients</a></p> <p><a href="#">Application and Device Control logs and quick reports</a></p>
<b>Compliance</b>	<p>The compliance logs contain information about client Host Integrity. No actions are associated with these logs.</p> <p><a href="#">Compliance log and quick report</a></p>
<b>Computer Status</b>	<p>The Computer Status log contains information about the real-time operational status of the client computers in the network.</p> <p>Available information includes the computer name, IP address, infected status, protection technologies, Auto-Protect status, versions, and definitions date. It also includes the user, last check-in time, policy, group, domain, and restart required status.</p> <p>You can also clear the infected status of computers from this log.</p> <p><b>Note:</b> This log contains information that is collected from both Windows clients and Mac clients.</p> <p><a href="#">Computer Status logs and reports</a></p>
<b>Deception</b>	<p>The Deception log contains information about any activity that the clients send back to Symantec Endpoint Protection Manager as the result of deceptor activity.</p> <p>Deception is a set of tools that you use to present to a potential attacker what appears to be desirable data and an attack vector. You use these tools to quickly detect and stop infiltration attempts. The Deception tools and help file are located in the /Tools/Deception folder of the installation file.</p> <p><a href="#">Monitors: Summary tab</a></p>
<b>Network and Host Exploit Mitigation</b>	<p>The Network and Host Exploit Mitigation logs contain information about intrusion prevention, the firewall, and Memory Exploit Mitigation.</p> <p>The logs contain information about attacks on the firewall and on intrusion prevention. Information is available about denial-of-service attacks, port scans, and the changes that were made to executable files. They also contain information about the connections that are made through the firewall (traffic), and the data packets that pass through. These logs also contain some of the operational changes that are made to computers, such as detecting network applications, and configuring software.</p> <p><a href="#">Network and Host Exploit Mitigation logs and quick reports</a></p>
<b>SONAR</b>	<p>The SONAR log contains information about the threats that have been detected during SONAR threat scanning. These are real-time scans that detect potentially malicious applications when they run on your client computers.</p> <p>The information includes items such as the time of occurrence, event actual action, user name, Web domain, application, application type, file, and path.</p> <p><a href="#">SONAR logs</a></p> <p><a href="#">About SONAR</a></p>

Log type	Contents and actions
<b>Risk</b>	The Risk log contains information about risk events. Available information includes the event time, event actual action, user name, computer, and domain, risk name and source, count, and file and path. <a href="#">Risk logs and quick reports</a>
<b>Scan</b>	The Scan log contains information about virus and spyware scan activity from both Windows clients and Mac clients. Available information includes items such as the scan start, computer, IP address, status, duration, detections, scanned, omitted, and domain. No actions are associated with these logs. <a href="#">Scan logs and quick reports</a>
<b>System</b>	The system logs contain information about events such as when services start and stop. No actions are associated with these logs. <a href="#">System logs and quick reports</a>

## Saving and deleting custom logs by using filters

You can construct custom filters by using the **Basic Settings** and **Additional Settings** to change the information that you want to see. You can save your filter settings to the database so that you can generate the same view again in the future. When you save your settings, they are saved in the database. The name you give to the filter appears in the **Use a saved filter** list box for that type of logs and reports.

In 12.1.x, **Additional Settings** is **Advanced Settings**.

### NOTE

If you selected **Past 24 hours** as the time range for a log filter, the 24-hour time range begins when you first select the filter. If you refresh the page, the start of the 24-hour range does not reset. If you select the filter, and wait to view a log, the time range starts when you select the filter. It does not start when you view the log.

If you want to make sure the past 24-hour range starts now, select a different time range and then reselect **Past 24 hours**.

1. To save a custom log by using a filter, in the main window, click **Monitors**.
2. On the **Logs** tab, select the type of log view that you want to configure a filter for from the **Log type** list box.
3. For some types of logs, a **Log content** list box appears. If it appears, select the log content that you want to configure a filter for.
4. In the **Use a saved filter** list box, select the filter that you want to start from. For example, select the default filter.
5. Under **What filter settings would you like to use**, click **Additional Settings**.

In 12.1.x, **Additional Settings** is **Advanced Settings**.

- 
6. Change any of the settings.
  7. Click **Save Filter**.
  8. In the dialog box that appears, in the **Filter name** box, type the name that you want to use for this log filter configuration. Only the first 32 characters of the name that you give display when the saved filter is added to the filter list.
  9. Click **OK** and your new filter name is added to the **Use a saved filter** list box.
  10. When the confirmation dialog box appears, click **OK**.
  11. To delete a saved filter, in the **Use a saved filter** list box, select the name of the log filter that you want to delete.
  12. Beside the **Use a saved filter** list box, click the **Delete** icon.
  13. When you are prompted to confirm that you want to delete the filter, click **Yes**.

## Viewing logs from other sites

If you want to view the logs from another site, you must log on to a server at the remote site from the Symantec Endpoint Protection Manager console. If you have an account on a server at the remote site, you can log on remotely and view that site's logs.

If you have configured replication partners, you can choose to have all the logs from the replication partners copied to the local partner and vice versa. If you choose to replicate logs, by default you see the information from both your site and the replicated sites when you view any log. If you want to see a single site, you must filter the data to limit it to the location you want to view. If you choose to replicate logs, be sure that you have sufficient disk space for the additional logs on all the replication partners.

### [How to install a second site for replication](#)

To view the logs from another site

1. Open a web browser.
2. Type the following in the address text box as follows:

```
http://SEPMServer:9090
```

Where SEPMServer is the server name or the IP address.

The IP address can be either IPv4 or IPv6. You must enclose the IPv6 address with square brackets: `http://[SEPMServer]:9090`

The console then downloads. The computer from which you log on must have the Java Runtime Environment (JRE) installed. If it does not, you are prompted to download and install it. Follow the prompts to install the JRE.

3. In the console logon dialog box, type your user name and password.
4. In the **Server** text box, if it does not fill automatically, type the server name or IP address and port number 8443 as follows:

```
http://SEPMServer:8443
```

5. Click **Log On**.

## Exporting data to a Syslog server

To increase the space in the database, you can configure the management server to send the log data to a Syslog server. When you export log data to a Syslog server, you must configure the Syslog server to receive the logs.

### [Exporting log data to a text file](#)

To export log data to a Syslog server:

1. In the console, click **Admin**.
2. Click **Servers**.
3. Click the local site or remote site that you want to export log data from.
4. Click **Configure External Logging**.
5. On the **General** tab, in the **Update Frequency** list box, select how often to send the log data to the file.
6. In the **Master Logging Server** list box, select the management server to send the logs to.  
If you use SQL Server and connect multiple management servers to the database, specify only one server as the Master Logging Server.
7. Check **Enable Transmission of Logs to a Syslog Server**.
8. Provide the following information:
  - **Syslog Server**  
Type the IP address or domain name of the Syslog server that you want to receive the log data.
  - **Destination Port**  
Select the protocol to use, and type the destination port that the Syslog server uses to listen for Syslog messages.
  - **Log Facility**  
Type the number of the log facility that you want to the Syslog configuration file to use, or use the default. Valid values range from 0 to 23.
9. On the **Log Filter** tab, check which logs to export.
10. Click **OK**.

## Exporting log data to a text file

When you export data from the logs to a text file, by default the files are placed in a folder. By default, that folder path is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\dump. Entries are placed in a .tmp file until the records are transferred to the text file.

### NOTE

You cannot restore the database by using exported log data.

The following table shows the correspondence of the types of log data to the names of the exported log data files. The log names do not correspond one-to-one to the log names that are used on the **Logs** tab of the **Monitors** page.

**Table 160: Log text file names for Symantec Endpoint Protection**

Log Data	Text File Name
Server Administration	scm_admin.log
Application and Device Control	agt_behavior.log
Server Client	scm_agent_act.log
Server Policy	scm_policy.log
Server System	scm_system.log
Client Packet	agt_packet.log
Client Proactive Threat	agt_proactive.log
Client Risk	agt_risk.log
Client Scan	agt_scan.log

Log Data	Text File Name
Client Security	agt_security.log
Client System	agt_system.log
Client Traffic	agt_traffic.log

#### NOTE

When you export to a text file, the number of exported records can differ from the number that you set in the **External Logging** dialog box. This situation arises when you restart the management server. After you restart the management server, the log entry count resets to zero, but there may already be entries in the temporary log files. In this situation, the first \*.log file of each type that is generated after the restart contains more entries than the specified value. Any log files that are subsequently exported contain the correct number of entries.

#### To export log data to a text file

1. In the console, click **Admin**.
2. Click **Servers**.
3. Click the local site or remote site that you want to configure external logging for.
4. Click **Configure External Logging**.
5. On the **General** tab, select how often you want the log data to be sent to the file.
6. In the **Master Logging Server** list box, select the server that you want to send logs to.  
If you use Microsoft SQL with more than one management server connecting to the database, only one server needs to be a Master Logging Server.
7. Check **Export Logs to a Dump File**.
8. If necessary, check **Limit Dump File Records** and type in the number of entries that you want to send at a time to the text file.
9. On the **Log Filter** tab, select all of the logs that you want to send to text files.  
If a log type that you select lets you select the severity level, you must check the severity levels that you want to export.
10. Click **OK**.

## Configuring a failover server for external logging

The Symantec Endpoint Protection Manager acts as a master logging server to forward logs to the syslog server. As of 14.3, you can set up a second management server to act as a failover server for the primary one. If the primary management server goes offline, the second management server takes over and forwards logs to the syslog server. When the primary management server comes back online, it resumes forwarding the logs.

#### To configure a failover server for external logging

1. In the console, click **Admin > Servers**, select the site, and click **Configure External Logging**.
2. On the **General** tab, in the **Master Logging Server** drop-down list, select the primary management server you want to send the logs to.  
If the primary server goes down, the next management server in the list takes over. The management servers are listed in the reporting server priority list on the **Admin > Servers > Edit Site Properties > General** tab.
3. Click **OK**.

[Installing a management server for failover and load balancing](#)

---

## Managing notifications

Notifications alert administrators and computer users about potential security problems.

Some notification types contain default values when you configure them. These guidelines provide reasonable starting points depending on the size of your environment, but they may need to be adjusted. Trial and error may be required to find the right balance between too many and too few notifications for your environment. Set the threshold to an initial limit, then wait for a few days. After a few days, you can adjust the notifications settings.

For virus, security risk, and firewall event detection, suppose that you have fewer than 100 computers in a network. A reasonable starting point in this network is to configure a notification when two risk events are detected within one minute. If you have 100 to 1000 computers, detecting five risk events within one minute may be a more useful starting point.

You manage notifications on the **Monitors** page. You can use the **Home** page to determine the number of unacknowledged notifications that need your attention.

[Notification management](#) lists the tasks you can perform to manage notifications.

**Table 161: Notification management**

Task	Description
Learn about notifications	Learn how notifications work. <a href="#">How notifications work</a>
Confirm that the email server is configured to enable email notifications	Notifications sent by email require that the Symantec Endpoint Protection Manager and the email server are properly configured. <a href="#">Establishing communication between the management server and email servers</a>
Review preconfigured notifications	Review the preconfigured notifications provided by Symantec Endpoint Protection. <a href="#">What are the types of notifications and when are they sent?</a>
View unacknowledged notifications	View and respond to unacknowledged notifications. <a href="#">Viewing and acknowledging notifications</a>
Configure new notifications	Optionally create notifications to remind you and other administrators about important issues. <a href="#">Setting up administrator notifications</a> <a href="#">About turning on notifications for remote clients</a>
Create notification filters	Optionally create filters to expand or limit your view of all of the notifications that have been triggered. <a href="#">Saving and deleting administrative notification filters</a>

## How notifications work

Notifications alert administrators and users about potential security problems. For example, a notification can alert administrators about an expired license or a virus infection.

Events trigger a notification. A new security risk, a hardware change to a client computer, or a trial license expiration can trigger a notification. Actions can then be taken by the system once a notification is triggered. An action might record the notification in a log, or run a batch file or an executable file, or send an email.

### NOTE

Email notifications require that communications between the Symantec Endpoint Protection Manager and the email server are properly configured.

You can set a damper period for notifications. The damper period specifies the time that must pass before the notification condition is checked for new data. When a notification condition has a damper period, the notification is only issued on the first occurrence of the trigger condition within that period. For example, suppose that a large-scale virus attack occurs, and that there is a notification condition configured to send an email whenever viruses infect five computers on the network. If

---

you set a damper period of one hour for that notification condition, the server sends only one notification email each hour during the attack.

#### NOTE

If you set the **Damper** period to **None** for notifications about critical events, you should make sure that clients can upload critical events immediately. The **Let clients upload critical events immediately** option is enabled by default and configured in the **Communications Settings** dialog box.

[Managing notifications](#)

[Establishing communication between the management server and email servers](#)

[What are the types of notifications and when are they sent?](#)

[Setting up administrator notifications](#)

[Viewing and acknowledging notifications](#)

## What are the types of notifications and when are they sent?

Symantec Endpoint Protection Manager provides notifications for administrators. You can customize most of these notifications to meet your particular needs. For example, you can add filters to limit a trigger condition only to specific computers. Or you can set notifications to take specific actions when they are triggered.

By default, some of these notifications are enabled when you install Symantec Endpoint Protection Manager. Notifications that are enabled by default are configured to log to the server and send email to system administrators.

[Managing notifications](#)

[How upgrades from another version affect notification conditions](#)

**Table 162: Preconfigured notifications**

Notification	Description
Authentication failure	A configurable number of logon failures in a defined period of time triggers the Authentication failure notification. You can set the number of logon failures and the time period within which they must occur to trigger the notification.
Client list changed	This notification triggers when there is a change to the existing client list. This notification condition is enabled by default. Client list changes can include: <ul style="list-style-type: none"><li>• The addition of a client</li><li>• A change in the name of a client</li><li>• The deletion of a client</li><li>• A change in the hardware of a client</li><li>• A change in the Unmanaged Detector status of a client</li><li>• A client mode change</li></ul>



Notification	Description
<b>Client security alert</b>	<p>This notification triggers upon any of the following security events:</p> <ul style="list-style-type: none"> <li>• Compliance events</li> <li>• Network and Host Exploit Mitigation events</li> <li>• Traffic events</li> <li>• Packet events</li> <li>• Device control events</li> <li>• Application control events</li> </ul> <p>You can modify this notification to specify the type, severity, and frequency of events that determine when these notifications are triggered.</p> <p>Some of these occurrence types require that you also enable logging in the associated policy.</p> <p><b>Note:</b> If you set the notification damper period to <b>None</b>, you should make sure that clients can upload critical events immediately. The <b>Let clients upload critical events immediately</b> option is enabled by default and configured in the <b>Communications Settings</b> dialog box.</p>
<b>Deception Detection</b>	<p>When an attacker attempts to touch or modify a deceptor, the Deception tools log an event. A notification is triggered when:</p> <ul style="list-style-type: none"> <li>• An attacker gets past the client's defenses.</li> <li>• An attacker retrieves information about the client computer.</li> <li>• An attacker attempts to use the client computer in additional attacks within the enterprise network.</li> </ul>
<b>Download Protection content out-of-date</b>	Alerts the administrators about out-of-date Download Protection content. You can specify the age at which the definitions trigger the notification.
<b>File reputation lookup alert</b>	<p>Alerts the administrators when a file is submitted to Symantec for a reputation check. SONAR and Download Insight use file reputation lookups and submit files to Symantec automatically.</p> <p>The <b>File Reputation Detection</b> notification is enabled by default.</p>
<b>Forced application detected</b>	This notification triggers when an application on the commercial application list is detected or when an application on the list of applications that the administrator monitors is detected.
<b>IPS signature out-of-date</b>	Alerts the administrators about out-of-date IPS signatures. You can specify the age at which the definitions trigger the notification.
<b>Licensing issue</b>	<p><b>Paid license expiration</b></p> <p>This notification alerts administrators and, optionally, partners, about the paid licenses that have expired or that are about to expire.</p> <p>This notification is enabled by default.</p> <p><b>Over-deployment</b></p> <p>This notification alerts administrators and, optionally, partners, about over-deployed paid licenses.</p> <p>This notification is enabled by default.</p> <p><b>Trial license expiration</b></p> <p>This notification alerts administrators about expired trial licenses and the trial licenses that are due to expire in 60, 30, and 7 days.</p> <p>This notification is enabled by default if there is a trial license. It is not enabled by default if your license is due for an upgrade or has been paid.</p>
<b>Memory Exploit Mitigation Detection</b>	This notification triggers when a Windows vulnerability attack is detected.
<b>Network load alert: requests for virus and spyware full definitions</b>	<p>Alerts the administrators when too many clients request a full definition set, and to potential network bandwidth issues.</p> <p>This notification is enabled by default.</p>
<b>New learned application</b>	This notification triggers when application learning detects a new application.

Notification	Description
<b>New risk detected</b>	This notification triggers whenever virus and spyware scans detect a new risk. <b>Note:</b> If you set the notification damper period to <b>None</b> , you should make sure that clients can upload critical events immediately. The <b>Let clients upload critical events immediately</b> option is enabled by default and configured in the <b>Communications Settings</b> dialog box.
<b>New software package</b>	This notification triggers when a new software package downloads or the following occurs: <ul style="list-style-type: none"> <li>• LiveUpdate downloads a client package.</li> <li>• The management server is upgraded.</li> <li>• The console manually imports client packages.</li> <li>• LiveUpdate has new security definitions or engine content.</li> </ul> You can specify whether the notification is triggered only by new security definitions, only by new client packages, or by both. This notification is enabled by default.
<b>New user-allowed download</b>	This notification triggers when a client computer allows an application that Download Insight detected. An administrator can use this information to help evaluate whether to block or allow the application.
<b>Power Eraser recommended</b>	Alerts the administrators when a regular scan cannot repair an infection, so the administrators can use Power Eraser. This notification is enabled by default.
<b>Risk outbreak</b>	This notification alerts administrators about security risk outbreaks. You set the number and type of occurrences of new risks and the time period within which they must occur to trigger the notification. Types of occurrences include occurrences on any computer, occurrences on a single computer, or occurrences on distinct computers. This notification condition is enabled by default. <b>Note:</b> If you set the notification damper period to <b>None</b> , you should make sure that clients can upload critical events immediately. The <b>Let clients upload critical events immediately</b> option is enabled by default and configured in the <b>Communications Settings</b> dialog box.
<b>Server health</b>	Server health issues trigger the notification. The notification lists the server name, the health status, the reason, and the last online or offline status. This notification is enabled by default.
<b>Single risk event</b>	This notification triggers upon the detection of a single risk event and provides details about the risk. The details include the user and the computer involved, and the actions that the management server took. <b>Note:</b> If you set the notification damper period to <b>None</b> , you should make sure that clients can upload critical events immediately. The <b>Let clients upload critical events immediately</b> option is enabled by default and configured in the <b>Communications Settings</b> dialog box.
<b>SONAR definitions out-of-date</b>	Alerts the administrators about out-of-date SONAR definitions. You can specify the age at which the definitions trigger the notification.
<b>System event</b>	This notification triggers upon certain system events and provides the number of such events that were detected. System events include management server activities, replication failures, backups, and system errors.
<b>Unmanaged computers</b>	This notification triggers when the management server detects unmanaged computers on the network. The notification provides details including the IP address, the MAC address, and the operating system of each unmanaged computer.
<b>Upgrade license expiration</b>	Upgrades from previous versions of Symantec Endpoint Protection Manager to the current version are granted an upgrade license. This notification triggers when the upgrade license is due to expire. This notification appears only after an upgrade.
<b>Virus definitions out-of-date</b>	Alerts the administrators about out-of-date virus definitions. You can specify the age at which the definitions trigger the notification. This notification is enabled by default.

---

## About partner notifications

When the management server detects that clients have paid licenses that are about to expire or that have expired, it can send a notification to the system administrator. Similarly, the management server can send a notification to the administrator when it detects that licenses are over-deployed.

However, in both of these cases, the resolution of the problem may require the purchase of new licenses or renewals. In many installations the server administrator may not have the authority to make such purchases, but instead relies upon a Symantec partner to perform this task.

The management server provides the ability to maintain the contact information for the partner. This information can be supplied when the server is installed. The system administrator can also supply or edit the partner information at any time after the installation in the Licenses pane of the console.

When the partner contact information is available to the management server, paid license-related notifications and over-deployed license notifications are sent automatically both to the administrator and to the partner.

[What are the types of notifications and when are they sent?](#)

## Establishing communication between the management server and email servers

For the management server to send automatic email notifications, you must configure the connection between the management server and the email server.

### [Managing notifications](#)

To establish communication between the management server and email servers

1. In the console, click **Admin**, and then click **Servers**.
2. Under **Servers**, select the management server for which you want to establish a connection to the email server.
3. Under **Tasks**, click **Edit the server properties**.
4. In the **Server Properties** dialog box, click the **Email Server** tab.
5. Enter the email server settings.

For details about setting options in this dialog box, click **Help**.

6. Click **OK**.

See [Sending test email messages fails in Endpoint Protection Manager console](#).

## Viewing and acknowledging notifications

You can view unacknowledged notifications or all notifications. You can acknowledge an unacknowledged notification. You can view all the notification conditions that are currently configured in the console.

The **Security Status** pane on the **Home** page indicates the number of unacknowledged notifications that have occurred during the last 24 hours.

### [Managing notifications](#)

1. To view recent unacknowledged notifications, in the console, click **Home**.
2. On the **Home** page, in the **Security Status** pane, click **View Notifications**.  
A list of recent unacknowledged notifications appears under the **Notifications** tab.

- 
3. Optionally, in the list of notifications, in the **Report** column, click the document icon if it exists.

The notification report appears in a separate browser window. If there is no document icon, all of the notification information appears in the **Message** column in the list of notifications.

4. To view all notifications, in the console, click **Monitors** and then click the **Notifications** tab.
5. Optionally, on the **Notifications** tab, from the **Use a saved filter** menu, select a saved filter.

#### [Saving and deleting administrative notification filters](#)

6. Optionally, on the **Notifications** tab, from the **Time range** menu, select a time range.
7. On the **Notifications** tab, click **View Notifications**.
8. To acknowledge a notification, view notifications.
9. On the **Notifications** tab, in the list of notifications, in the **Ack** column, click the red icon to acknowledge the notification.
10. To view all configured notification conditions, in the console, click **Monitors**.
11. On the **Monitors** page, on the **Notifications** tab, click **Notification Conditions**.

All the notification conditions that are configured in the console are shown. You can filter the list by selecting a notification type from the **Show notification type** menu.

## Saving and deleting administrative notification filters

You can use filters to expand or limit your view of administrative notifications in the console. You can save new filters and you can delete previously saved filters.

#### [Viewing and acknowledging notifications](#)

#### [Managing notifications](#)

You can create a saved filter that uses any combination of the following criteria:

- **Time range**
- **Acknowledged status**
- **Notification type**
- **Created by**
- **Notification name**

For example, you can create a filter that only displays unacknowledged risk outbreak notifications posted during the past 24 hours.

1. To add a notification filter, in the console, click **Monitors**.
2. On the **Monitors** page, on the **Notifications** tab, click **Additional Settings**.

In 12.1.x, **Additional Settings** is **Advanced Settings**.

- 
3. Under the **What filter settings would you like to use?** heading, set the criteria for the filter.
  4. Click **Save Filter**.
  5. On the **Notifications** tab, in the **Filter name** box, type a filter name, and then click **OK**.
  6. To delete a saved notification filter, in the console, click **Monitors**.
  7. On the **Monitors** page, on the **Notifications** tab, on the **Use a saved filter** menu, choose a filter.
  8. At the right of the **Use a saved filter** menu, click the **X** icon.
  9. In the **Delete Filter** dialog box, click **Yes**.

## Setting up administrator notifications

You can configure notifications to alert you and other administrators when particular kinds of events occur. You can also add the conditions that trigger notifications to remind you to perform important tasks. For example, you can add a notification condition to inform you when a license has expired, or when a security risk has been detected.

When a notification triggers, it can perform specific actions, such as the following:

- Log the notification to the database.
- Send an email to one or more individuals.
- Run a batch file.

### NOTE

To send email notifications, you must configure a mail server to communicate with the management server.

### [Establishing communication between the management server and email servers](#)

You choose the notification condition from a list of available notification types.

Once you choose the notification type, you then configure it as follows:

- Specify filters.  
Not all notification types provide filters. When they do, you can use the filters to limit the conditions that trigger the notification. For example, you can restrict a notification to trigger only when computers in a specific group are affected.
- Specify settings.  
All notification types provide settings, but the specific settings vary from type to type. For example, a risk notification may let you specify what type of scan triggers the notification.
- Specify actions.  
All notification types provide actions you can specify.

### NOTE

If you set the **Damper** period to **None** for notifications about critical events, you should make sure that clients can upload critical events immediately. The relevant notifications include the following: **Client security alert**, **Single risk event**, **New risk detected**, and **Risk outbreak**. The **Let clients upload critical events immediately** option is enabled by default and configured in the **Communications Settings** dialog box.

To set up an administrator notification

- 
1. In the console, click **Monitors**.
  2. On the **Monitors** page, on the **Notifications** tab, click **Notification Conditions**.
  3. On the **Notifications** tab, click **Add**, and then click a notification type.
  4. In the **Add Notification Condition** dialog box, provide the following information:
    - In the **Notification name** text box, type a name to label the notification condition.
    - Under **What filter settings would you like to use**, if it is present, specify the filter settings for the notification condition.
    - Under **What settings would you like for this notification**, specify the conditions that trigger the notification.
    - Under **What should happen when this notification is triggered**, specify the actions that are taken when the notification is triggered.
  5. Click **OK**.

[Managing notifications](#)

[Viewing and acknowledging notifications](#)

## How upgrades from another version affect notification conditions

When Symantec Endpoint Protection is installed on a new server, many of the preconfigured notification conditions are enabled by default. An upgrade to Symantec Endpoint Protection from a previous version, however, can affect which notification conditions are enabled by default. It can also affect their default settings.

The following notification conditions are enabled by default in a new installation of Symantec Endpoint Protection:

- **Client list changed**
- **New client software**
- **Over deployment issue**
- **Paid license issue**
- **Risk outbreak**
- **Server health**
- **Trialware license expiration**
- **Virus definitions out-of-date**

When an administrator upgrades the software from a previous version, all existing notification conditions from the previous version are preserved. However, existing **New software package** notification conditions become **New client software** notification conditions. The **New client software** condition has two settings that are not present in the **New software package** condition: **Client package** and **Security definitions**. When the software is upgraded, both of these settings are enabled for notification conditions of this type that are preserved across the upgrade. **New client software** notifications that are conditions created after the upgrade, however, have the **Client package** setting enabled and the **Security definitions** setting disabled by default.

### NOTE

When the **Security definitions** setting in the **New client software** notification condition is enabled, it may cause a large number of notifications to be sent. This situation can occur when there are many clients or when there are frequently scheduled security definition updates. If you do not want to receive frequent notifications about security definition updates, you can edit the notification condition to disable the **Security definitions** setting.

Several notification conditions may have a new setting that did not appear in earlier versions: **Send email to system administrators**. If that setting is new for a notification condition, it is disabled by default for any existing condition of that type following the upgrade.

---

When a default notification condition type has not been added in a previous installation, that notification condition is added in the upgraded installation. However, the upgrade process cannot determine which default notification conditions may have been deleted deliberately by the administrator in the previous installation. With one exception, therefore, all of the following action settings are disabled in each default notification condition in an upgraded installation: **Send email to system administrators**, **Log the notification**, **Run batch file**, and **Send email to**. When all four of these actions are disabled, the notification condition is not processed, even though the condition itself is present. Administrators can edit the notification conditions to enable any or all of these settings.

Note that the **New client software** notification condition is an exception: it can produce notifications by default when it is added during the upgrade process. Unlike the other default notification conditions, both the **Log the notification** and the **Send email to system administrators** action settings are enabled for this condition.

If the previous version of the software does not support licenses, an **Upgrade license expiration** notification condition is enabled.

Some notification condition types are not available in previous versions of the software. Those notification conditions are enabled by default when the software is upgraded.

[What are the types of notifications and when are they sent?](#)

---

# Managing management servers, sites, and databases

---

Learn about client-server communication, performing disaster recovery, and configuring replication, sites, and failover

Use this section to:

- Configure the connection between the management server and the client.
- Configure management servers and certificates.
- Manage the database.
- Set up failover and load balancing.
- Manage sites and replication.
- Perform disaster recovery.

## About the types of Symantec Endpoint Protection servers

The following definitions may be helpful to understand when managing servers:

- **Site**  
A site consists of one or more management servers and one database typically located together at the same business location. The site to which you log on is the local site, and you can modify it directly. Any site other than the local site is referred to as a remote site. You connect sites by using replication.  
[Setting up sites and replication](#)
- **Management server**  
The computer on which the Symantec Endpoint Protection Manager software is installed. From the management server, policies can be created and assigned to different organizational groups. You can monitor clients, view reports, logs, and alerts, and configure servers and administrator accounts. Multiple management servers at a single site provide failover and load balancing capabilities.  
[Setting up failover and load balancing](#)
- **Database server**  
The database used by Symantec Endpoint Protection Manager. There is one database per site, either the Microsoft SQL Server Express or the Microsoft SQL Server. The database can be on the same computer as the management server or on a different computer if you use a SQL Server database. SQL Server Express replaced the embedded database in 14.3 RU1.  
[Maintaining the database](#)
- **Replication partner**  
A relationship created between two sites to enable data replication between them.  
[Setting up sites and replication](#)

## Exporting and importing server settings

The server properties file includes the server settings for Symantec Endpoint Protection Manager. You may need to export and import the server properties file in the following situations:

- You use the disaster recovery file to reinstall Symantec Endpoint Protection Manager.  
The disaster recovery file does not include the server settings. When you reinstall Symantec Endpoint Protection Manager, you lose any default server settings that you had previously changed. You can use the exported server properties file to reimport the changed server settings.
- You install Symantec Endpoint Protection Manager in a test environment and later install the management server in a production environment. You can import the exported server properties file to the production environment.



---

## Managing Symantec Endpoint Protection Manager servers and third-party servers

1. To export server settings, in the console, click **Admin**, and then click **Servers**.
2. Under **Servers**, expand **Local Site (Site site\_name)**, and then select the management server you want to export.
3. Click **Export Server Properties**.
4. Select a location in which to save the file and specify a file name.
5. Click **Export**.
6. To import server settings, in the console, click **Admin**, and then click **Servers**.
7. Under **Servers**, expand **Local Site (Site site\_name)**, and then select the management server for which you want to import settings.
8. Click **Import Server Properties**.
9. Select the file you want to import, and then click **Import**.
10. Click **Yes**.

## Managing Symantec Endpoint Protection Manager servers and third-party servers

You can configure Symantec Endpoint Protection Manager to integrate with many of the different types of servers in your network environment.

**Table 163: Server management**

Task	Description
Learn about servers	Decide which types of servers you need to set up. <a href="#">About the types of Symantec Endpoint Protection servers</a>
Set server communication permissions	You can allow or deny access to the remote console. You manage access by adding exceptions based on the IP address of a single computer or a group of computers. <a href="#">Granting or blocking access to remote Symantec Endpoint Protection Manager consoles</a>
Modify server settings	To modify database settings, or to restore your database on a different computer, you can modify server settings. <a href="#">Reinstalling or reconfiguring Symantec Endpoint Protection Manager</a>
Configure the mail server	To work with a specific mail server in your network, you need to configure the mail server. <a href="#">Establishing communication between the management server and email servers</a>
Manage directory servers	You can integrate Symantec Endpoint Protection with directory servers to help manage administrator accounts or to create organizational units. <a href="#">Connecting Symantec Endpoint Protection Manager to a directory server</a>
Configure proxy settings if you use a proxy server to connect to Symantec LiveUpdate servers	To set up the Symantec Endpoint Protection Manager to connect to the Internet through a proxy server, you must configure the proxy server connection. <a href="#">Configuring Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate</a>
Import or export server properties	You can export server settings to an xml file, and you can re-import the same settings. <a href="#">Exporting and importing server settings</a>

Task	Description
Manage server certificates	<p>The Symantec Endpoint Protection Manager server uses a server certificate to encrypt data for the communication between all servers, and clients in a network. The server identifies and authenticates itself with a server certificate. You may need to back up, update, or generate a new server certificate.</p> <p><a href="#">About server certificates</a></p> <p><a href="#">Updating or restoring a server certificate</a></p> <p><a href="#">Backing up a server certificate</a></p> <p><a href="#">Generating a new server certificate</a></p>
Configure SecurID Authentication for a server	<p>If you choose to authenticate administrator accounts by using RSA SecurID, you must also configure the management server to communicate with the RSA server.</p> <p><a href="#">Using RSA SecurID authentication with Symantec Endpoint Protection Manager</a></p>
Configure two-factor authentication for Symantec Endpoint Protection Manager with Symantec VIP	<p>If you use Symantec VIP in your environment for two-factor authentication, you can enable it for those administrators who authenticate with Symantec Endpoint Protection Manager Authentication. This support is added in version 14.2.</p> <p><a href="#">Configuring two-factor authentication with Symantec VIP</a></p>
Move the server to a different computer	<p>You may need to move the management server software from one computer to another for the following reasons:</p> <ul style="list-style-type: none"> <li>• You must move the management server from a test environment to a production environment.</li> <li>• The computer on which the management server runs has a hardware failure.</li> </ul> <p>You can move the management server software in the following ways:</p> <ul style="list-style-type: none"> <li>• Install the management server on another computer and perform replication. <a href="#">How to install a second site for replication</a></li> <li>• Install the management server on another computer using the recovery file. <a href="#">Reinstalling or reconfiguring Symantec Endpoint Protection Manager</a></li> </ul>
Start and stop the management server	<p>The management server runs as an automatic service. You must stop the management server service when you upgrade, or perform disaster recovery.</p> <p><a href="#">Stopping and starting the management server service</a></p>

## Maintaining the database

Symantec Endpoint Protection (SEPM) supports both the Microsoft SQL Server Express database and the Microsoft SQL Server database. If you have more than 5,000 clients, use a Microsoft SQL Server database.

Symantec Endpoint Protection Manager automatically installs the Microsoft SQL Server Express database. You can also install SQL Server Express separately. The database contains information about security policies, configuration settings, attack data, logs, and reports. SQL Server Express replaced the embedded database in 14.3 RU1.

After you install Symantec Endpoint Protection Manager, the management server may start to slow down after a few weeks or a few months. To improve the management server performance, you may need to reduce the database storage space and schedule various database maintenance tasks.

**Table 164: Database management tasks**

Task	Description
Schedule regular database backups	<p>You should schedule regular database backups in case the database gets corrupted.</p> <p><a href="#">Backing up the database and logs</a></p> <p><a href="#">Scheduling automatic database backups</a></p> <p><a href="#">Disaster recovery best practices for Endpoint Protection</a></p> <p>Optionally, to prevent an automatic sweep of the database until after a backup occurs, you can manually sweep data from the database.</p> <p><a href="#">Clearing log data from the database manually</a></p>
Schedule database maintenance tasks	<p>You can speed up the interaction time between the management server and the database by scheduling database maintenance tasks. You can schedule the management server to perform the following maintenance tasks immediately or when users are not on the client computers.</p> <ul style="list-style-type: none"> <li>• Remove unused data from the transaction log.</li> <li>• Rebuild the database table indexes to improve the database's sorting and searching capabilities.</li> </ul> <p><a href="#">Scheduling automatic database maintenance tasks</a></p>
Periodically check the database file size	<p>Make sure that the database does not reach the maximum file size. The Microsoft SQL Server Express database has a 10 GB size limit. If you install SQL Server Express when you install SEPM, SEPM warns you if you approach the limit.</p> <p><a href="#">Increasing the Microsoft SQL Server database file size</a></p>
Calculate the database storage space that you need	<p>Before you can decide how to reduce the amount of storage space, calculate the total amount of disk space that you need.</p> <p><b>The database storage is based on the following factors:</b></p> <ul style="list-style-type: none"> <li>• Log size and expiration time period.</li> <li>• The number of client computers.</li> <li>• The average number of viruses per month.</li> <li>• The number of events you need to retain for each log.</li> <li>• The number of content updates.</li> </ul> <p>The content updates require about 300 MB each.</p> <p><a href="#">Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager</a></p> <p><a href="#">Reverting to an older version of the Symantec Endpoint Protection security updates</a></p> <ul style="list-style-type: none"> <li>• The number of client versions you need to retain for each language.</li> </ul> <p>For example, if you have both 32-bit clients and 64-bit clients, you need twice the number of language versions.</p> <ul style="list-style-type: none"> <li>• The number of backups you need to keep.</li> </ul> <p>The backup size is approximately 75 percent of the database size, and then multiplied by the number of backup copies that you keep.</p> <p>For more information on how to calculate the hard disk space you need, see the Symantec white paper, <a href="#">Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper</a>.</p>

Task	Description
Reduce the volume of log data	<p>The database receives and stores a constant flow of entries into its log files. You must manage the data that is stored in the database so that the stored data does not consume all the available disk space. Too much data can cause the computer on which the database runs to crash.</p> <p><b>You can reduce the volume of log data by performing the following tasks:</b></p> <ul style="list-style-type: none"> <li>• Upload only some of the client logs to the server, and change the frequency with which the client logs are uploaded. <a href="#">Specifying client log size and which logs to upload to the management server</a></li> <li>• Specify how many log entries the client computer can keep in the database, and how long to keep them. <a href="#">Specifying the log size and how long to keep log entries in the database</a></li> <li>• Filter the less important risk events and system events out so that less data is forwarded to the server. <a href="#">Modifying log handling and notification settings on Windows computers</a></li> <li>• Reduce the amount of space in the directory where the log data is stored before being inserted into the database. <a href="#">About increasing the disk space on the server for client log data</a></li> <li>• Reduce the number of clients that each management server manages. <a href="#">Configuring a management server list for load balancing</a></li> <li>• Reduce the heartbeat frequency, which controls how often the client logs are uploaded to the server. <a href="#">Updating policies and content on the client using push mode or pull mode</a></li> </ul>
Export log data to another server	<p>For security purposes, you might need to retain the number of log records for a longer period of time. To keep the client log data volume low, you can export the log data to another server. You can configure multiple management servers to receive log data in case one server goes down.</p> <p><a href="#">Exporting data to a Syslog server</a> <a href="#">Exporting log data to a text file</a></p>
Create client installation packages with only the protection that you need	<p>The more protection features that you install with the client, the more space that the client information takes in the database. Create the client installation package with only the appropriate level of protection the client computer needs. The more groups you add, the more space the client information takes in the database.</p> <p><a href="#">Choosing which security features to install on the client</a></p>
Use the Group Update Provider to download content	<p>If you have low bandwidth or more than 100 client computers, use Group Update Providers to download content. For example, 2,000 clients using a Group Update Provider is the equivalent of using four to five management servers to download content.</p> <p><a href="#">Using Group Update Providers to distribute content to clients</a></p> <p>To reduce disk space and database size, you can reduce the number of content revisions that are kept on the server.</p> <p><a href="#">Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager</a></p>
Restore the database	<p>You can recover a corrupted database by restoring the database on the same computer on which it was installed originally. Or, you can install the database on a different computer.</p> <p><a href="#">Restoring the database</a></p>

### [Verifying the connection with the database](#)

The information in the database is stored in tables, also called the database schema. You might need the schema to write queries for customized reports. For more information, see the:

[Symantec Endpoint Protection Manager Database Schema Reference](#)

## Running automatic database backups

You can schedule database backups to occur at a time when fewer users are logged on to the network.

---

You can also back up the database at any time.

### Backing up the database and logs

1. In the console, click **Admin > Servers**.
2. Under **Servers**, click **Local Site (My Site) > SQLEXPRESSSYMC**.
3. Under **Tasks**, click **Edit Database Properties**.
4. In the **Database Properties** dialog box, on the **Backup Settings** tab, do the following tasks.
  - In the **Backup server** drop-down list, specify on which management server you want to save the backup.
  - Check **Back up logs** if you need to save a copy of the logs for security purposes or company policy. Otherwise, leave this option disabled, as logs use a lot of disk space.
  - Set the **Number of backups to keep** if your company policy requires it. Keep the number low if you use the default database and your database size is too large.
5. Make sure **Schedule Backups** is checked, and set the schedule.
6. Click **OK**.

## Scheduling automatic database maintenance tasks

After you install the management server, the space in the database grows continually. The management server slows down after a few weeks or months. To reduce the database size and to improve the response time with the database, the management server performs the following database maintenance tasks:

- Truncates the transaction log.  
The transaction log records almost every change that takes place within the database. The management server removes unused data from the transaction log.
- Rebuilds the index.  
The management server defragments the database table indexes to improve the time it takes to sort and search the database.

By default, the management server performs these tasks on a schedule. You can perform the maintenance tasks immediately, or adjust the schedule so that it occurs when users are not on their computers.

### NOTE

You can also perform the database maintenance tasks in Microsoft SQL Server Management Studio. However, you should perform these tasks in either Symantec Endpoint Protection Manager or Management Studio, but not both.

1. To run database maintenance tasks on demand, in the console, click **Admin**, and then click **Servers**.
2. Under **Servers**, click the icon that represents the database.
3. Under **Tasks**, select either of the following options:
  - **Truncate Transaction Log Now**
  - **Rebuild Indexes Now**

- 
4. Click **Run**.
  5. After the task completes, click **Close**.
  6. To schedule database maintenance tasks to run automatically, in the console, click **Admin**, and then click **Servers**.
  7. Under **Servers**, click the icon that represents the database.
  8. Under **Tasks**, click **Edit Database Properties**.
  9. On the **General** tab, check either or both of the following options, then click **Schedule Task** and specify the schedule for each task.
    - **Truncate the database transaction logs**. The default schedule for this task is every four hours.
    - **Rebuild Indexes**. The default schedule for this task is every Sunday at 2:00.

#### **WARNING**

If you perform these tasks in SQL Server Management Studio, uncheck these options.

#### [Scheduling automatic database backups](#)

### **Increasing the Microsoft SQL Server database file size**

If you use the SQL Server database, periodically check the database size to make sure that the database does not reach its maximum size. If you can, increase the maximum size that the SQL Server database holds.

#### [Scheduling automatic database maintenance tasks](#)

To increase the Microsoft SQL Server database size

1. On the Microsoft SQL server computer, open the SQL Server Management Studio.
2. In the Object Explorer, Expand the "Databases" folder, right-click **sem5**, and click **Properties**.
3. In the **Database Properties** dialog box, select **Files**.
4. Under **Database files**, select **sem5\_log1**, and scroll to the right to view the **Autogrowth** column.
5. In the **Autogrowth** column, click the ... button.
6. In the **Change Autogrowth for sem5\_log1** dialog box, click **Unrestricted File Growth**, and then click **OK**.
7. Click **OK**.

### **Specifying client log size and which logs to upload to the management server**

Company policy might require you to increase the time and type of log events that the database keeps. You can specify the number of log entries that are kept, and the number of days that each entry is kept on the client.

You can configure whether to upload each type of client log to the server. You can also configure the maximum upload size. If you choose not to upload the client logs, you cannot perform the following tasks:

- You cannot view the client log data from the Symantec Endpoint Protection Manager console by using the **Logs** tab on the **Monitors** page.
- You cannot back up the client logs when you back up the database.
- You cannot export the client log data to a file or a centralized log server.

#### **NOTE**

Some client log settings are group-specific and some are set in the Virus and Spyware Protection policy, which can be applied to a location. If you want all remote client log and office client log settings to differ, you must use groups instead of locations to manage remote clients.

#### [Specifying the log size and how long to keep log entries in the database](#)

---

To specify client log size and which logs to upload to the management server

1. On the console, click **Clients**, and select a group.
2. On the **Policies** tab, click **Client Log**.
3. In the **Client Log Settings** for group name dialog box, set the maximum file size and the number of days to keep log entries.
4. Check **Upload to management server** for any logs that you want the clients to forward to the server.
5. For the **Security** log and **Traffic** log, set the damper period and the damper idle period.
6. Click **OK**.

## Specifying the log size and how long to keep log entries in the database

To help control hard disk space, you can decrease the number of log entries that the database keeps. You can also configure the number of days the entries are kept.

### NOTE

Log information on the Symantec Endpoint Protection Manager console **Logs** tab on the **Monitors** page is presented in logical groups for you to view. The log names on the **Site Properties Log Settings** tab correspond to log content rather than to log types on the **Monitors** page **Logs** tab.

### [Specifying client log size and which logs to upload to the management server](#)

To specify the log size and how long to keep log entries in the database

1. In the console, click **Admin**.
2. Under **Servers**, expand **Local Site**, and click the database.
3. Under **Tasks**, click **Edit Database Properties**.
4. On the **Log Settings** tab, set the number of entries and number of days to keep log entries for each type of log.
5. Click **OK**.

## About increasing the disk space on the server for client log data

A configuration that uploads a large volume of client log data to the server at frequent intervals can cause disk space problems on the server. If you must upload a large volume of client log data, you may have to adjust some default values to avoid these space problems. As you deploy to clients, you should monitor the space on the server in the log insertion directory and adjust these values as needed.

The default directory where the logs are converted to .dat files and then written to the database is in the following default location:

```
C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\inbox\log.
```

To adjust the values that control the space available on the server, you must change these values in the Windows registry. The Windows registry keys that you need to change are located on the server in HKEY\_LOCAL\_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM.

[Windows registry keys that contain log upload settings](#) lists the Windows registry keys and their default values and describes what they do.

**Table 165: Windows registry keys that contain log upload settings**

Value name	Description
MaxInboxSpace	Specifies the space that is allotted for the directory where log files are converted to .dat files before they are stored in the database. The default value is 8 GB.
MinDataFreeSpace	Specifies the minimum amount of space that should be kept free in this directory. This key is useful to ensure that other applications that use the same directory have enough space to run without an adverse effect on performance. The default value is 200 MB.
IntervalOfInboxSpaceChecking	Specifies how long the management server waits before it checks on the amount of space in the inbox that is available for log data. The default value is 30 seconds.

### Maintaining the database

## Clearing log data from the database manually

You can perform a manual log sweep after backing up the database, if you prefer to use this method as part of routine database maintenance.

If you allow an automatic sweep to occur, you may lose some log data if your database backups do not occur frequently enough. If you regularly perform a manual log sweep after you have performed a database backup, it ensures that you retain all your log data. This procedure is very useful if you must retain your logs for a relatively long period of time, such as a year. You can manually clear the logs, but this procedure is optional and you do not have to do it.

### Backing up the database and logs

#### Specifying the log size and how long to keep log entries in the database

To clear log data from the database manually

1. To prevent an automatic sweep of the database until after a backup occurs, increase a site's log size to their maximums.
2. Perform the backup, as appropriate.
3. On the computer where the manager is installed, open a Web browser and type the following URL:

`https://localhost:8443/servlet/ConsoleServlet?ActionType=ConfigServer&action=SweepLogs`

After you have performed this task, the log entries for all types of logs are saved in the alternate database table. The original table is kept until the next sweep is initiated.

4. To empty all but the most current entries, perform a second sweep. The original table is cleared and entries then start to be stored there again.
5. Return the settings on the **Log Settings** tab of the **Site Properties** dialog box to your preferred settings.

## Setting up failover and load balancing

The client computers must be able to connect to a management server at all times to download the security policy and to receive log events. You should set up failover to maintain communication with a Symantec Endpoint Protection Manager when the management server becomes unavailable. Load balancing is used to distribute client management between multiple management servers using a management server list.

The following table lists the tasks that you should perform to set up failover and load balancing.



**Table 166: Process for setting up failover and load balancing**

Tasks	Description
Read about failover and load balancing.	You should understand if and when you need to set up management servers for failover and load balancing. <a href="#">About failover and load balancing</a>
Install additional management servers.	<a href="#">Installing a management server for failover or load balancing</a> The number of clients for each management server depends on several factors, such as the log sizes. To calculate how many management servers you need, see: <a href="#">Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper</a>
Add management servers to a management server list.	To set up load balancing, you add multiple management servers to a management server list. You can either use the default management server list or add management servers to a new management server list. A management server list includes the IP addresses or host names of management servers to which clients can connect. <a href="#">Configuring a management server list for load balancing</a>
Assign the custom management server list to a group.	After you have created a custom management server list, you must assign the management server list to a group. <a href="#">Assigning a management server list to a group and location</a>

### [Setting up sites and replication](#)

If the management server goes offline, or the client and the management server do not communicate, you should also troubleshoot the problem.

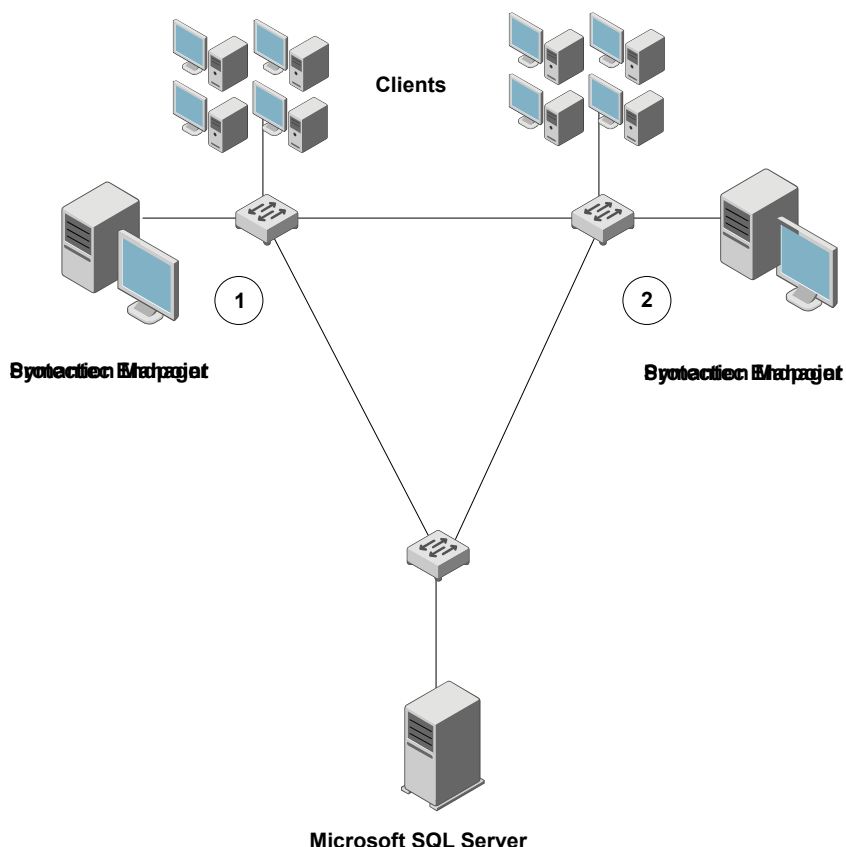
[Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)

## About failover and load balancing

You can install two or more management servers that communicate with one database and configure them for failover or load balancing.

Load balancing occurs with a prioritized list of management servers that is assigned to a group. You should add at least two management servers to a site to automatically distribute the load among them. You can install more management servers than are required to handle your clients to protect against the failure of an individual management server. In a custom management server list, each server is assigned to a priority level. A client that comes onto the network selects a priority one server to connect to at random. If the first server it tries is unavailable and there are other priority one servers in the list, it randomly tries to connect to another. If no priority one servers are available, then the client tries to connect to one of the priority two servers in the list. This method of distributing client connections randomly distributes the client load among your management servers.

The following diagram shows components on different subnets. Management servers and database servers can be on the same subnets. The servers are identified with the numbers 1 and 2, which signify a failover configuration.



In a failover configuration, all clients send traffic to and receive traffic from server 1. If server 1 goes offline, all clients send traffic to and receive traffic from server 2 until server 1 comes back online. The database is illustrated as a remote installation, but it also can be installed on a computer that runs the Symantec Endpoint Protection Manager.

You may also want to consider failover for content updates, if you intend to use local servers. All the components that run LiveUpdate can also use a prioritized list of update sources. Your management servers can use a local LiveUpdate server and failover to LiveUpdate servers in other physical locations.

#### **NOTE**

The use of internal LiveUpdate servers, Group Update Providers, and site replication does not provide load balancing functionality. You should not set up multiple sites for load balancing.

#### **NOTE**

In 14.3 MPx and earlier, you can set up failover and load balancing if you use a Microsoft SQL Server database only. You can set up failover with the embedded database, but only if you use replication. When you use replication with an embedded database, Symantec recommends that you do not configure load balancing, as data inconsistency and loss may result.

[Setting up failover and load balancing](#)

[Configuring a management server list for load balancing](#)

[Determining how many sites you need](#)

[Setting up sites and replication](#)

---

## Configuring a management server list for load balancing

By default, the management servers are assigned the same priority when configured for failover and load balancing. If you want to change the default priority after installation, you can do so by using the Symantec Endpoint Protection Manager console. You can only configure load balancing when a site includes more than one management server.

Load balancing occurs between the servers that are assigned to priority 1 in a management server list. If more than one server is assigned to priority 1, the clients randomly choose one of the servers and establish communication with it. If all priority 1 servers fail, clients connect with the server assigned to priority 2.

### To provide both load balancing and roaming:

- Enable DNS and put a domain name as the only entry in a custom management server list.
- Enable the Symantec Endpoint Protection location awareness feature and use a custom management server list for each location. Create at least one location for each of your sites.
- Use a hardware device that provides failover or load balancing. Many of these devices also offer a setup for roaming.

### [About failover and load balancing](#)

To configure a management server list for load balancing

1. In the console, click **Policies**.
2. Expand **Policy Components**, and then click **Management Server Lists**.
3. Under **Tasks**, click **Add a Management Server List**.
4. In the **Management Server Lists** dialog box, click **Add > New Server**.
5. In the **Add Management Server** dialog box, in the **Server Address** box, type the fully qualified domain name or IP address of a management server.

If you type an IP address, be sure that it is static, and that all clients can resolve it.

6. Click **OK**.
7. Add any additional servers.
8. To configure load balancing with another management server, click **Add > New Priority**.
9. To change the priority of a server for load balancing, select a server, and then click **Move Up** or **Move Down**.
10. Click **OK**.

You must then apply the management server list to a group.

### [Assigning a management server list to a group and location](#)

## Installing a management server for failover or load balancing

Failover configurations are used to maintain communication when clients cannot communicate with a Symantec Endpoint Protection Manager. Load balancing is used to distribute client management between management servers. You can configure failover and load balancing by assigning priorities to management servers in management server lists.

Failover and load balancing installations are supported only when the original Symantec Endpoint Protection Manager uses a Microsoft SQL Server database. The SQL Server Native Client files also must be installed on the computer that you use for failover or load balancing.

### To install a management server for failover or load balancing:

1. Install a Symantec Endpoint Protection Manager.

### [Installing Symantec Endpoint Protection Manager](#)

- 
2. In the **Management Server Configuration Wizard** panel, check **Custom Configuration**, and then click **Next**.  
[Configuring Symantec Endpoint Protection Manager after installation](#)
  3. Select the number of clients you expect the server to manage, and then click **Next**.
  4. Check **Install an additional management server to an existing site**, and then click **Next**.
  5. In the server information panel, accept or change the default values, and then click **Next**.
  6. In the **Microsoft SQL Server Information** dialog box, click **OK** in the message about installing the SQL Server client tools.
  7. Enter the remote server values for the following text boxes:  
**Step One** tells the Symantec Endpoint Protection Manager where to find the SQL Server on the network, which includes host name, instance name, and port.  
You also pick the authentication type, including Windows Authentication or SQL authentication.
    - **Database server**instance\_name  
SQL server port  
Database name  
**SQL client folder** (on the local computer)  
If this text box does not automatically populate with the correct path, the Microsoft SQL Client Utility is not installed or it is not installed correctly.
  8. **Step Two** tells the Symantec Endpoint Protection Manager how to authenticate to the SQL Server and includes the database name, database user, and database user's password.  
You should have had this information available already for when you installed the first management server for that site.
  9. Click **Next**.
  10. Specify and confirm a password for the Symantec Endpoint Protection Manager admin account.  
Optionally, provide an administrator email address.
  11. Click **Next**.
  12. At the warning, read the text message, and then click **OK**.
  13. In **Management Server Completed** panel, click **Finish**.

[Configuring a failover server for external logging](#)

## Assigning a management server list to a group and location

After you add a policy, you must assign it to a group or a location or both. You can also use the management server list to move a group of clients from one management server to another.

You must have finished adding or editing a management server list before you can assign the list.

---

### Configuring a management server list for load balancing

1. To assign a management server list to a group and location, in the console, click **Policies**.
2. In the **Policies** page, expand **Policy Components**, and then click **Management Server Lists**.
3. In the **Management Server Lists** pane, select the management server list you want to assign.
4. Under **Tasks**, click **Assign the List**.
5. In the **Apply Management Server List** dialog box, check the groups and locations to which you want to apply the management server list.
6. Click **Assign**.
7. Click **Yes**.
8. To assign a management server list to a group or location on the Clients page, in the console, click **Clients > Policies**.
9. On the **Policies** tab, select the group, and then uncheck **Inherit policies and settings from parent group**.  
You cannot set any communication settings for a group unless the group no longer inherits any policies and settings from a parent group.
10. Under **Location-independent Policies and Settings**, click **Communication Settings**.
11. In the **Communication Settings for group name** dialog box, under **Management Server List**, select the management server list.  
The group that you select then uses this management server list when communicating with the management server.
12. Click **OK**.

## Setting up sites and replication

A site consists of one database, one or more management servers, and clients. By default, you deploy Symantec Endpoint Protection as a single site. Organizations with more than one data center or physical location generally use multiple sites.

Replication configurations are used for redundancy. Data from one database is duplicated, or replicated, on another database. If one database fails, you can still manage and control all clients because the other database contains the client information.

### What are sites and how does replication work?

**Table 167: Process for setting up sites and replication**

Tasks	Description
Step 1: Determine whether you need to add another site	Before you set up multiple sites and replication, make sure that it is necessary. Symantec recommends that you set up multiple sites only in specific circumstances and that you add a maximum of five sites in each site farm. If you do add an additional site, decide which site design works for your organization. <a href="#">Deciding whether or not to set up multiple sites and replication</a> <a href="#">Determining how many sites you need</a>
Step 2: Install Symantec Endpoint Protection Manager on the first site	When you install Symantec Endpoint Protection for the first time, by default you have installed the first site, or the local site. <a href="#">Installing Symantec Endpoint Protection Manager</a>

Tasks	Description
Step 3: Install Symantec Endpoint Protection Manager on the second site	<p>You create a second site by installing a second management server. The second site is classified as a remote site and the management server is called a replication partner. Replication occurs according to the default schedule that when you added the second site during the initial installation. After you have added a replication partner, you can change the replication schedule and what data is replicated.</p> <p><a href="#">How to install a second site for replication</a></p> <p>The first time that the databases between the two sites replicate, let the replication finish completely. The replication may take a long time because the entire database gets replicated.</p> <p>You may want to replicate the data immediately, rather than waiting until the database are scheduled to replicate. You can also change the replication schedule to occur earlier or later.</p> <p>If you upgrade the management server on one site, you must upgrade the management server version on all sites.</p> <p><a href="#">Replicating data immediately</a></p>
Step 4: Check the history for replication events (optional)	<p>If you need to check that the replication occurred or to troubleshoot the replication events, look at the System log.</p> <p>In the second management server, view the System log. Filter for the <b>Administrative &gt; Replication events</b> event type.</p> <p><a href="#">Viewing logs</a></p>

You can also reconfigure a management server to replicate the data with a currently existing site in your network. Or, if you have two non-replicating sites, you can convert one of the sites into a site that replicates with the second site.

#### [Reinstalling or reconfiguring Symantec Endpoint Protection Manager](#)

- After you configure the Symantec Endpoint Protection, you should back up the database, which contains all your configuration changes.  
[Backing up the database and logs](#)
- If you disable a replication partner to upgrade to the latest version of the management server, you must re-add the replication partner.  
[Disabling replication and restoring replication before and after an upgrade](#)  
[Upgrading to a new release](#)

#### [Connecting to a directory server on a replicated site](#)

## What are sites and how does replication work?

### [Sites and replication partners](#)

### [How does replication work?](#)

### [Determining the size of the replication server](#)

#### **Sites and replication partners**

A site is a Symantec Endpoint Protection Manager database with one or more Symantec Endpoint Protection Managers attached to that database. Replication enables data to be duplicated between databases on separate sites so that both databases contain the same information. If one database fails, you can manage each site by using the information on the database from the second site.

A replication partner is an individual management server within the second site, or remote site. A site may have as many replication partners as needed. Each partner connects to the main site or local site, which is the site that you are logged on to. All sites that are set up as partners are considered to be in the same site farm.

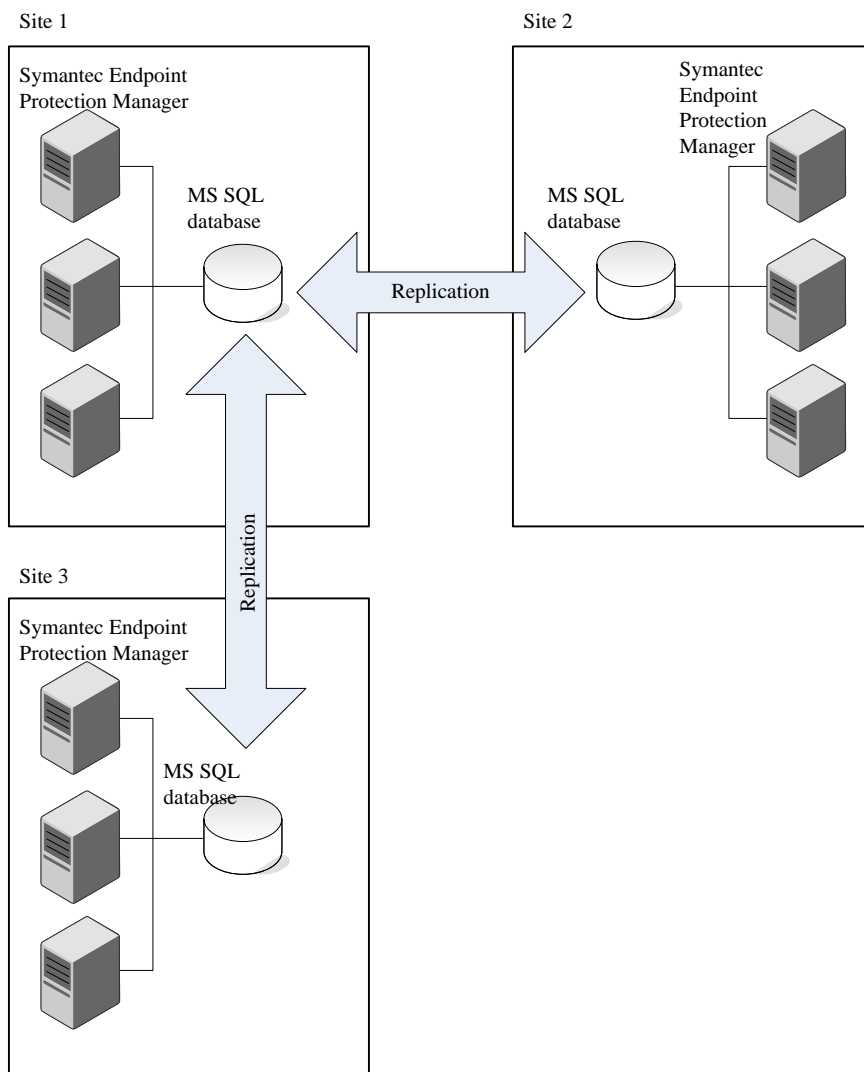
Each site you replicate data with is either a replication partner or a site partner. Both replication partners and site partners use multiple management servers, but the database they use and the way in which they communicate is different:

- Replication partners can use either the default database (Microsoft SQL Server Express in 14.3 RU1) or a Microsoft SQL Server database. The management servers do not share the database. All replication partners share a common license key. If you use the Microsoft SQL Server database, you can connect multiple management servers that share one database. Only one of the management servers needs to be set up as a replication partner.
- Site partners share a single Microsoft SQL Server database.

### How does replication work?

The changes that you make on any partner are duplicated to all other partners. For example, you may want to set up one site at your main office (site 1) and a second site (site 2). Site 2 is a partner to site 1. The databases on site 1 and site 2 are reconciled by using the replication schedule. If a change is made on site 1, it automatically appears on site 2 after replication occurs. If a change is made on site 2, it automatically appears on site 1 after replication occurs. You can also install a third site (site 3) that can replicate data from either site 1 or site 2.

After replication occurs, the database on site 1 and the database on site 2 are the same. Only computer identification information for the servers differs.



For more information on how often to replicate, see the following article: [The Philosophy of SEPM Replication Setup](#)  
[Deciding whether or not to set up multiple sites and replication](#)

---

[Determining how many sites you need](#)

[How to resolve data conflicts between sites during replication](#)

### **Determining the size of the replication server**

A replication partner requires a larger database than a single management server installation. The increased size requirements for the replication server include the following factors:

- Number of managed clients
- Client installation package sizes retained in the database
- Number of log files retained
- Database maintenance settings
- Log size and expiration timeframes
- Definition update sizes
- Database backup information requirements

In general, the hard disk requirements for the replication server should be at least three times the hard disk space used by the original Symantec Endpoint Protection Manager for the initial replication.

[How to install a second site for replication](#)

[Replication considerations and best practices](#)

[Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper](#)

## **How to resolve data conflicts between sites during replication**

Replication causes data to be transferred or forwarded to another management server. Sites can have multiple replication partners, and any changes made on one partner are replicated to all sites.

### **What data is duplicated?**

Neither replication site overrides the other. Instead they compare what each site has, and if one site has a package or piece of content the other does not, then it is shared. If all LiveUpdate content and client packages match up, then nothing is exchanged.

The replication partners duplicate the following data:

- Policies and groups (required bidirectional)
- LiveUpdate content and client installation packages, if you specify these options (optional bidirectional)
- Logs (optional bidirectional or unidirectional)

If you upgrade the management server on one site, you must upgrade the management server version on all sites. Replication does not occur if the database schema versions do not match.

The following table describes how the management server resolves conflicts if administrators change settings on the sites in a site farm.



**Table 168: How the management server resolves conflicts between sites**

Conflict type	Example	Resolution
Two differences cannot exist together.	Administrators for site 1 and site 2 both configure an identical Firewall policy setting. On site 1, the setting is enabled. On site 2, the setting is disabled.	The management server retains only the most recently made change. For example, if you made a change on site 1 first, and site 2 second, then the site 2 change is retained.
The same variable is created for both sites.	Administrators on site 1 and site 2 both add a group with the same name.	The management server retains both changes, adding a tilde and the numeral 1 (~1) after the more recently made variable. For example, with two groups named as Sales, the most recently named Sales group becomes Sales ~1.
Data can merge without conflict.	The administrator for site 1 adds two Firewall policies and the administrator for site 2 adds five Firewall policies.	The management server merges the changes. For example, the management server displays all seven Firewall policies on both sites.

## Deciding whether or not to set up multiple sites and replication

Before you install a second site, you should decide whether or not multiple sites and replication are a good choice in your network. Setting up more than one site adds a complexity that you may not need. Multiple sites can cause certain tasks such as viewing client logs and reports more difficult. Generally, you should install only one site.

The main purposes to set up multiple sites and replication are:

- If your network has a slow WAN link.  
Multiple sites provide a second management server to which clients in multiple geographical areas can connect locally. For example, suppose a company has several large offices in both Germany and in the United States. If the connection between Germany and the United States is slow, then the company should create one site in Germany and one site in the United States. The Germany clients can connect to the Germany site and the United States clients can connect to the United States site. This distribution reduces the number of clients that have to communicate over the slow WAN link.
- For database redundancy.  
Replication ensures that if one datacenter was corrupted or lost, you would have backed up the database in a different datacenter.

In some situations, you should use a Group Update Provider (GUP) instead of multiple sites and replication. Use a GUP when you have either a lot of clients, or clients that are distributed over several geographical locations.

### NOTE

You should not set up more than five replicated sites.

**Table 169: Deciding whether to use more than one site with replication, a GUP, or neither**

Question	Answer	Use multiple sites with replication or use a GUP
Do you have more than 45,000 clients?	Yes. Do you have either multiple locations or a slow WAN link that connects to a location with more than 1,000 clients?	Yes. <ul style="list-style-type: none"> <li>• For a slow WAN link, consider using replication.</li> <li>• For multiple locations, consider using a GUP.</li> </ul>
		No. You do not need either replication or a GUP.

Question	Answer	Use multiple sites with replication or use a GUP
	No.	Yes. Consider using replication.
	Do you have a slow WAN link that connects to a location with more than 1,000 clients?	No. You do not need either replication or a GUP.
Do you have a slow WAN link?	Yes.	Yes. Consider using replication.
	Do you have multiple locations with more than 1,000 clients per location?	No. Consider using a GUP.
	No.	Yes. Consider using replication.
	Do you have multiple locations with more than 1,000 clients per location?	No. You do not need either replication or a GUP.
Do you have multiple locations with more than 1,000 clients per location?	Yes.	Yes. Consider using a GUP.
	Do you have a slow WAN link that connects to a location with more than 1,000 clients?	No. You do not need either replication or a GUP.
	No	Yes. Consider using a GUP.
	Do you have a slow WAN link that connects to a location with more than 1,000 clients?	No. You do not need either replication or a GUP.

[When to use replication with Symantec Endpoint Protection Manager](#)

[Using Group Update Providers to distribute content to clients](#)

[Setting up sites and replication](#)

[Determining how many sites you need](#)

## Determining how many sites you need

A majority of small and medium-sized organizations need only a single site to centrally manage network security. Since each site has only one database, all data is centrally located.

Even a large organization with a single geographic location typically needs only needs one site. But for the organizations that are too complex to manage centrally, you should use a distributed management architecture with multiple sites.

**You should consider multiple sites for any of the following factors:**

- A large number of clients.
- The number of geographical locations and the type of communications links between them.
- The number of functional divisions or administrative groups.
- The number of datacenters. A best practice is to set up one Symantec Endpoint Protection site for each datacenter.
- How frequently you want to update the content.
- How much client log data you need to retain, how long you need to retain it, and where it should be stored.
- A slow WAN link between multiple physical locations with thousands of clients. If you set up a second site with its own management server, you can minimize the client-server traffic over that slow link. With fewer clients, you should use a Group Update Provider.

[Using Group Update Providers to distribute content to clients](#)

- Any miscellaneous corporate management and IT security management considerations that are unique.

**Use the following size guidelines to decide how many sites to install:**

- Install as few sites as possible, up to a maximum of 20 sites. You should keep the number of replicated sites under five.
- Connect up to ten management servers to a database.
- Connect up to 18,000 clients (for 14.x) or 50,000 clients (for 12.1.x) to a management server.

---

After you add a site, you should duplicate site information across multiple sites by replication. Replication is the process of sharing information between databases to ensure that the content is consistent.

**Table 170: Multi-site designs**

Site design	Description
Distributed	Each site performs replication bi-directionally for groups and policies, but not logs and content. To view the site reports, you use the console to connect to a management server in the remote site. Use this design when you do not need immediate access to remote site data.
Centralized logging	All logs are forwarded from the other sites to a central site. Use this design when you require centralized reporting.
High availability	Each site has multiple management server installations and database clustering. To handle additional clients, you add multiple management servers rather than adding multiple sites. You then use a management server list to configure client computers to automatically switch to an alternative management server if the primary management server becomes unavailable. You use this design to provide redundancy, failover, and disaster recovery.  <b>Note:</b> When you use replication with an embedded database (14.3 MPx and earlier), Symantec recommends that you do not add load balancing, as data inconsistency and loss may result.  <a href="#">Setting up failover and load balancing</a>

For more information on whether or not to set up replication, see the following article: [When to use replication with Symantec Endpoint Protection Manager](#)

[What are sites and how does replication work?](#)

[Setting up sites and replication](#)

[Deciding whether or not to set up multiple sites and replication](#)

## How to install a second site for replication

Installing a second site for replication is a two-part process:

- Install a second Symantec Endpoint Protection Manager and database to replicate with a Symantec Endpoint Protection Manager and database that is already installed.
- Log on to the second Symantec Endpoint Protection Manager and change the schedule and the items that you want to replicate (optional).

[Changing the replication frequency and content](#)

### Installing a second site for replication

1. Install a second Symantec Endpoint Protection Manager.  
[Installing Symantec Endpoint Protection Manager](#)  
The **Management Server Configuration Wizard** automatically starts after the management server installation.
2. In the **Management Server Configuration Wizard**, click **Custom configuration for new installation (more than 500 clients, or custom settings)**, and then click **Next**.
3. Click **Install an additional site**, and then click **Next**.
4. In the next panel, type the following information, and then click **Next**:
  - **Replication server**  
The name or IP address of the management server that is already installed and that this management server replicates with.
  - **System Administrator name** and **Password**.

---

The system administrator's user name is `admin` by default. You must use a system administrator account, and not a limited administrator account or domain administrator account.

- Check **Replicate client packages and LiveUpdate content between the local site and this partner site** (Optional).

If you don't check this option now, you can check it later.

5. If a warning message about accepting the certificate appears, click **Yes**.
6. In the site information pane, accept or change the default values, and then click **Next**.
7. In the database choice pane, click either the **Default SQL Server Express database** or **Microsoft SQL Server database**, and then click **Next**.

Symantec recommends that the site with which you replicate uses the same type of database, but it is not required. For 14.3 MPx and earlier, the default database is the **Default Embedded database**.

Complete the installation based on the database that you choose.

8. In the **Run LiveUpdate** pane, click **Next**.  
Optionally add the partner information.
9. Optionally accept the data collection feature, and then click **Next**.  
The database gets created. This step takes some time.  
The Symantec Endpoint Protection Manager launches.

Change the schedule, if necessary. [Changing the replication frequency and content](#)

[Setting up sites and replication](#)

[What are sites and how does replication work?](#)

[Deciding whether or not to set up multiple sites and replication](#)

[Preventing replication during an upgrade](#)

## Changing the replication frequency and content

By default, replication is scheduled to occur automatically after you install the second site and management server. Replication occurs according to the default schedule as part of installing the second management server. However, you may need to change the frequency based on how long replication takes. You can change the frequency on either the local site or the new site, but Symantec recommends that you configure replication on the new site first. The schedule on both sites is the same the next time the two sites replicate. The site with the smaller ID number initiates the scheduled replication. Whichever site is configured as the new replication partner always has its database overwritten by the database from the local site that the new site points to.

Both sites automatically share groups and policies. You can choose whether to replicate logs, client installation packages, or LiveUpdate content based on the amount of disk space that is available.

The time that it takes to replicate depends on the size of the database as well as network connection between the sites. First, test a replication cycle to see how long it takes. You should schedule your replication based on that time period, and make sure that the time when the management servers duplicate data does not overlap. Both the client packages and LiveUpdate content can include a large volume of data. The data in a client package might be as large as 5 GB. The client installation packages may require as much as 500 MB of disk space. If you plan to replicate logs, make sure that you have sufficient disk space for the additional logs on all the replication partner servers.

After the initial, full database replication, subsequent replications are fairly small, if you only replicate policies, clients, and groups, and not logs. Make sure that the management servers have enough available disk space to replicate based on the frequency and content.

### To change the replication frequency and schedule:

1. In the console, click **Admin > Servers**.
2. Under **Servers > Local Site**, expand **Replication Partners**, and select the site you want to replicate with.

- 
3. Under **Tasks**, click **Edit Replication Partner Properties**.
  4. Choose the content you want to replicate.
  5. To change the schedule, do one of the following tasks:
    - Check **Auto-replicate** to let the management server choose when to replicate the data.  
This option causes frequent and automatic replication to occur between two sites, about every 2 hours.
    - Check **Replicate on a schedule** to set up a custom schedule.
  6. Click **OK**.

#### [Replication considerations and best practices](#)

## Replicating data immediately

Replication normally occurs according to the default schedule when you set up an additional site. You might want replication to occur immediately. The site with the smaller ID number initiates the scheduled replication.

If you use the Microsoft SQL Server database with more than one server, you can only initiate replication from the first server at that site.

1. In the console, click **Admin > Servers**.
2. Under **Servers > Local Site**, expand **Replication Partners** and select the site.
3. Under **Tasks**, click **Replicate Now**.
4. Click **Yes**, and then **OK**.

#### [Changing the replication frequency and content](#)

#### [Setting up sites and replication](#)

## Deleting sites

Deleting a replication partner disconnects the partnership in Symantec Endpoint Protection Manager, but does not uninstall the management server software or delete the second site.

If you remove the management server at a remote site, you need to manually delete it from all sites. Uninstalling the software from one management server console does not make the icon disappear from the **Servers** pane on other consoles.

#### [Disabling replication and restoring replication before and after an upgrade](#)

To delete a site

1. In the console, click **Admin > Servers > Local Site**, expand **Replication Partners**, right-click the replication partner, and click **Delete Replication Partner**.
2. Under **Remote Sites**, right-click the site and click **Delete Remote Site**.
3. Click **Yes**.

#### [Setting up sites and replication](#)

## Disaster recovery best practices for Endpoint Protection

To prepare for recovery after a hardware failure or database corruption, you should back up the information that is collected after you install Symantec Endpoint Protection Manager.

#### [Preparing for disaster recovery](#)

#### [Performing disaster recovery](#)

#### **Preparing for disaster recovery**

**Table 171: High-level steps to prepare for disaster recovery**

Step	Description
Step 1: Back up the database	Back up the database regularly, preferably weekly. By default, the database backup folder is saved to the following default location: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\backup The backup file is called date_timestamp.zip. <a href="#">Backing up the database and logs</a>
Step 2: Back up the disaster recovery file	The recovery file includes the encryption password, keystore files domain ID, certificate files, license files, and port numbers. By default, the file is located in the following directory: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Server Private Key Backup\recovery_timestamp.zip The recovery file only stores the default domain ID. If you have multiple domains, the recovery file does not store that information. If you need to perform disaster recovery, you must re-add the domains. <a href="#">Adding a domain</a>
Step 3: Update or back up the server certificate (optional)	If you update the self-signed certificate to a different certificate type, the management server creates a new recovery file. Because the recovery file has a timestamp, you can tell which file is the latest one. <a href="#">Updating or restoring a server certificate</a> <a href="#">Backing up a server certificate</a>
Step 4: Save the IP address and host name of the management server to a text file (optional)	If you have a catastrophic hardware failure, you must reinstall the management server using the IP address and host name of the original management server. Add the IP address and host name to a text file, such as: Backup.txt.
Step 5: Store the backup data in a secure location off-site	Copy the files you backed up in the previous steps to another computer

### Performing disaster recovery

[Process for performing disaster recovery](#) lists the steps to recover your Symantec Endpoint Protection environment in the event of hardware failure or database corruption.

Before you follow these steps, make sure that you made backups and recovery files.

**Table 172: Process for performing disaster recovery**

Step	Action
Step 1: Reinstall Symantec Endpoint Protection Manager using a disaster recovery file.	By reinstalling the management server, you can recover the files that were saved after initial installation. <a href="#">Reinstalling or reconfiguring Symantec Endpoint Protection Manager</a> If you reinstall Symantec Endpoint Protection Manager on a different computer and without using the disaster recovery file, you must generate a new server certificate. <a href="#">Generating a new server certificate</a>
Step 2: Restore the database.	You can restore the database with or without a database backup. <a href="#">Restoring the database</a>
Step 3: Re-enable Federal Information Processing Standards (FIPS) 140-2 compliance. (optional)	If you use a FIPS-compliant version of Symantec Endpoint Protection and have FIPS compliance enabled, after you recover Symantec Endpoint Protection Manager, you must reenable FIPS compliance. This setting is not stored in the disaster recovery file.

### [Backing up your license files](#)

---

## Exporting and importing server settings

See: [Disaster recovery best practices for Endpoint Protection](#).

## Backing up the database and logs

Symantec recommends that you back up the database at least weekly. You should store the backup file on another computer.

By default, the backup file is saved in the following folder: `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\backup`.

The backups are placed in a .zip file. By default, the backup database file is named `date_timestamp.zip`, the date on which the backup occurs.

### NOTE

Avoid saving the backup file in the product installation directory. Otherwise, the backup file is removed when the product is uninstalled.

Log data is not backed up unless you configure Symantec Endpoint Protection Manager to back it up. If you do not back up the logs, then only your log configuration options are saved during a backup. You can use the backup to restore your database, but the logs in the database are empty of data when they are restored.

You can keep up to 10 versions of site backups. You should ensure that you have adequate disk space to keep all your data if you choose to keep multiple versions.

You can check the System log as well as the backup folder for the status during and after the backup.

You can back up the database immediately, or schedule the backup to occur automatically.

### NOTE

The Microsoft SQL Server Express database has a 10 GB limit. To back up the database, you cannot have more than 10 GB in the database and you must have at least 10 GB of available disk space. [Best practices for upgrading from the embedded database to the Microsoft SQL Server Express database](#)

## Scheduling automatic database backups

---

## Disaster recovery best practices for Endpoint Protection

1. To back up the database and logs, on the computer that runs Symantec Endpoint Protection Manager, on the **Start** menu, click **All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Tools > Database Back Up and Restore**.
2. In the **Database Back Up and Restore** dialog box, click **Back Up**.
3. In the **Back Up Database** dialog box, optionally check **Backup logs**, and then click **Yes**.
4. Click **OK**.
5. When the database backup completes, click **Exit**.
6. Copy the backup database file to another computer.
7. To back up the database and logs from within the console, in the console, click **Admin > Servers**.
8. Under **Servers**, click **Local Site (My Site) > SQLEXPRESSSYMC** (as of 14.3 RU1) or **localhost**.
9. Under **Tasks**, click **Back Up Database Now**.
10. In the **Back Up Database** dialog box, optionally check **Backup logs**, and then click **Yes**.
11. Click **OK**.
12. Click **Close**.

## Backing up a server certificate

In case the computer on which the management server is installed gets corrupted, you should back up the private key and the certificate.

The JKS Keystore file is backed up during the initial installation. A file that is called `server_timestamp.xml` is also backed up. The JKS Keystore file includes the server's private and public key pair and the self-signed certificate.

To back up a server certificate

1. In the console, click **Admin**, and then click **Servers**.
2. Under **Servers**, click the management server whose server certificate you want to back up.
3. Under **Tasks**, click **Manage Server Certificate**, and then click **Next**.
4. In the **Manage Server Certificate** panel, click **Back up the server certificate** and then click **Next**.
5. In the **Back Up Server Certificate** panel, click **Browse** to specify a backup folder, and then click **Open**.

Note that you back up the management server certificate into the same folder.

6. In the **Backup Server Certificate** panel, click **Next**.
7. Click **Finish**.

## About server certificates

### Generating a new server certificate

### Best practices for updating server certificates and maintaining the client-server connection

## Reinstalling or reconfiguring Symantec Endpoint Protection Manager

If you need to reinstall or reconfigure the management server, you can import all your settings by using a disaster recovery file. You can reinstall the software on the same computer, in the same installation directory. Symantec Endpoint Protection Manager creates a recovery file during installation. You can also use this procedure to reconfigure the existing site, or to install an additional site for replication.



---

## Disaster recovery best practices for Endpoint Protection

1. To reinstall the management server, uninstall the existing management server.
2. Install the server from the installation file.

### Installing Symantec Endpoint Protection Manager

3. In the **Welcome** panel, make sure that the **Use a recovery file to restore communication with previously deployed clients** option is checked, and then click **Next**.

By default, the recovery file is located in: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Server Private Key Backup. The recovery file reconnects your clients to the Symantec Endpoint Protection Manager.

4. Follow the instructions in each panel. The default settings work for most cases. If the reinstalled server connects to an existing database, you change the database settings to those of the existing database.

You can also restore the database if necessary. However, if the Symantec Endpoint Protection Manager database resides on another computer or is otherwise not affected, you do not need to restore your database.

### Restoring the database

5. To reconfigure the management server, click **Start > All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Tools > Management Server Configuration Wizard**.
6. Select one of the following options:
  - To reconfigure the management server on the existing site, click **Reconfigure the management server**.
  - To reconfigure the management server to replicate data with an existing site, click **Reconfigure the management server to replicate with a different site**.

This option reconfigures the locally installed management server to create a new site and to replicate the data with another existing site in your network. Also, if you have two non-replicating sites, use this option to convert one of the sites into a site that replicates with the second site.

#### NOTE

If you leave **Use a recovery file to restore communication with previously deployed clients** checked, the installation proceeds. However, it ignores the default domain ID in the recovery file and uses the domain ID of the replication partner. After reconfiguration completes, existing clients may fail to connect due to the change in domain ID.

7. Follow the instructions in each panel.

## Reinstalling or reconfiguring Symantec Endpoint Protection Manager

### Generating a new server certificate

You generate a new server certificate for Symantec Endpoint Protection Manager if the IP address or host name of the server changes, or if your private key was compromised.

By default, client-server communication depends on verifying the server certificate. If you generate a new server certificate, this verification fails and communication is interrupted. Follow the best practices for updating the certificate before you begin this procedure.

### Best practices for updating server certificates and maintaining the client-server connection

To generate a new server certificate

- 
1. In the console, click **Admin**, and then click **Servers**.
  2. Under **Servers**, click the management server.
  3. Under **Tasks**, click **Manage Server Certificate**, and then click **Next**.
  4. In the **Manage Server Certificate** panel, click **Generate new server certificate**. Make sure that **Generate new Keys** is checked, and then click **Next**.

**Generate new Keys** generates a new certificate with a new key pair (public and private keys). If you uncheck this option, the new certificate uses the same key pair as before, which lowers the Symantec Endpoint Protection Manager server security profile in the case of a compromised key pair.

5. Click **Yes**, and then click **Next**.
6. You must restart the following services to use the new certificate:
  - The Symantec Endpoint Protection Manager service
  - The Symantec Endpoint Protection Manager Webserver service
  - The Symantec Endpoint Protection Manager API service(As of 14)

[Stopping and starting the management server service](#)

[Stopping and starting the Apache Web server](#)

The next time you log on to Symantec Endpoint Protection Manager, you are asked to trust the new certificate.

[About accepting the self-signed server certificate for Symantec Endpoint Protection Manager](#)

[Logging on to the Symantec Endpoint Protection Manager console](#)

## Restoring the database

If the database gets corrupted or you need to perform disaster recovery, you can restore the database. To restore the database, you must first have backed it up.

[Backing up the database and logs](#)

### NOTE

You must restore the database using the same version of Symantec Endpoint Protection Manager that you used to back up the database. You can restore the database on the same computer on which it was installed originally or on a different computer.

The database restore might take several minutes to complete.

### To restore the database with a database backup:

1. Stop the management server service.  
[Stopping and starting the management server service](#)
2. On the **Start** menu, click **All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Tools > Database Back Up and Restore**.
3. In the **Database Back Up and Restore** dialog box, click **Restore**.
4. Click **Yes** to confirm the database restoration.
5. In the **Restore Site** dialog box, select the backup database file, and then click **OK**.
6. Locate the copy of the backup database file that you made when you backed up the database. By default, the backup database file is named date\_timestamp.zip.
7. Click **OK**.
8. Click **Exit**.
9. Restart the management server service.

---

### To restore the database without a database backup:

You may need to restore the database without a database backup in the following cases:

- You tried and cannot reset your administrator password.  
[Resetting a forgotten Symantec Endpoint Protection Manager password](#)
  - You did not make a database backup and the database is corrupted.
1. Back up the policy files.  
You import the exported policy files after you reinstall the database.
  2. If you have multiple domains, create a text file named SEPBackup.txt and add any domain IDs. (Optional)  
To save the management server information, add the IP address and host name of the management server to the file.
  3. Stop the management server service.  
[Stopping and starting the management server service](#)
  4. Reconfigure the management server using the Management Server Configuration Wizard and the recovery file.  
[Reinstalling or reconfiguring Symantec Endpoint Protection Manager](#)
  5. On the reconfigured Symantec Endpoint Protection Manager, in the following file:  
`SEPM_Install/tomcat/etc/conf.properties`  
The default for SEPM\_Install is C:/Program files (x86)/Symantec/Symantec Endpoint Protection Manager.  
Change:  
`scm.agent.groupcreation=false` to `scm.agent.groupcreation=true`  
This edit enables the automatic creation of client groups. Otherwise, the clients to reappear in the default group as they check in.  
Clients can communicate with Symantec Endpoint Protection Manager, but only re-appear in the console only after their next check-in.

---

## Managing clients and policies from the Symantec Endpoint Security cloud console

---

Learn how to manage clients and policies from both the ICDm cloud console and the Symantec Endpoint Protection Manager.

To take advantage of some policy features in the cloud, you can set up hybrid management in your environment. With hybrid management, you enroll a Symantec Endpoint Protection Manager (SEPM) domain in the ICDm console. You can then manage your client computers and some policies from the ICDm cloud console and Symantec Endpoint Security.

### What is Symantec Endpoint Security (SES) and the Integrated Cyber Defense Manager (ICDm) cloud console?

Symantec Endpoint Security (SES) is the fully cloud-managed version of the on-premises Symantec Endpoint Protection, which delivers multilayer protection to stop threats regardless of how they attack your endpoints. You manage Symantec Endpoint Security through the Symantec Integrated Cyber Defense Manager (ICDm), a unified cloud console that provides threat visibility across your endpoints and leverages multiple technologies to manage the security posture of your organization.

The ICDm is the management console for the cloud that is equivalent to the on-premises Symantec Endpoint Protection Manager (SEPM) management console. Both management consoles manage the same client, called the Symantec Agent in the cloud and the Symantec Endpoint Protection client in the SEPM.

#### [What is Symantec Endpoint Security?](#)

#### [Symantec Endpoint Security Complete](#)

You can manage your devices and some policies from Symantec Endpoint Security, and manage the rest of the protection from the Symantec Endpoint Protection Manager. This hybrid-managed option provides some additional security features that the on-premises Symantec Endpoint Protection Manager does not provide.

The Symantec Endpoint Protection 14.0.1 (14.1) and later clients are cloud-enabled (called the Symantec Agent on Symantec Endpoint Security). You use the same client for either SEP or SES.

To use hybrid management, after you install Symantec Endpoint Protection Manager, you enroll each Symantec Endpoint Protection Manager domain in the ICDm cloud console.

The following is a high-level summary of the features you get when you enroll a Symantec Endpoint Protection Manager domain:

- Discover and block suspicious detections with the Intensive Protection policy
- Product configuration to optimize for low-bandwidth environments
- Integrated false positive management with a central allow list and deny list
- Modern cloud console for managing advanced features

#### [Choosing between the on-premises management, hybrid management, or cloud management options](#)

---

## Choosing between the on-premises management, hybrid management, or cloud-only management options

The Symantec Endpoint Protection 14.0.1 (14.1) agent or later are the agent versions that Symantec Endpoint Security (Endpoint Security) manages. These agents are cloud-enabled and you can manage them from either Symantec Endpoint Protection Manager (SEPM) or the Integrated Cyber Defense Manager cloud console.

You can manage the agents from the cloud only, on-premises only, or a combination of both (hybrid management):

- For cloud management only, you use the Symantec Integrated Cyber Defense Manager (ICDm), a unified cloud console. You must purchase either Symantec Endpoint Security Enterprise or Symantec Endpoint Security Complete.
- For on-premises management, you install the Symantec Endpoint Protection Manager, which is the management console for Symantec Endpoint Protection. You can purchase Symantec Endpoint Protection, Symantec Endpoint Security Enterprise, or Symantec Endpoint Security Complete.
- For hybrid management, you use the Symantec Endpoint Protection Manager for on-premises managed devices and the ICDm console to manage cloud-managed devices. You enroll each Symantec Endpoint Protection Manager domain in the ICDm cloud console. Enrollment gives you a single view of all devices and alerts in ICDm. In addition, you can manage your devices and some policies from ICDm for your entire hybrid deployment. However, you can manage the rest of the protection for your on-premises devices from the Symantec Endpoint Protection Manager. You must purchase Symantec Endpoint Security Enterprise or Symantec Endpoint Security Complete.

**Table 173: Deciding whether to use the on-premises Symantec Endpoint Protection or the cloud-managed Symantec Endpoint Security**

If you want to...	Use this product
Manage clients entirely using the cloud console	<p><b>Symantec Endpoint Security (Enterprise or Complete)</b></p> <p>The cloud only management console is the Integrated Cyber Defense Manager (ICDm) and the devices use Symantec Agents version 14.2 RU1 or later. You create and deploy the agent installation package from Symantec Endpoint Security. You install the on-premises client software on the devices, as before.</p> <p>You manage the agents completely from the cloud, which bypasses communication with the on-premises management console, Symantec Endpoint Protection Manager.</p> <p>Use this approach in the following situations:</p> <ul style="list-style-type: none"> <li>• You do not want the cost or overhead of installing and managing a management server and database.</li> <li>• You have multiple Symantec enterprise products and want to share management capabilities across a single management console.</li> <li>• You want unified visibility into threats, policies and incidents from multiple Symantec products, which reduces incident response times from days to minutes.</li> <li>• Symantec Endpoint Security has additional features that Symantec Endpoint Protection on-premises does not have.</li> </ul> <p><a href="#">Quick reference for Symantec Endpoint Protection-managed versus Symantec Endpoint Security-managed features in ICDm</a></p> <p>To manage your agents from the cloud, you log on to your Symantec Security cloud account directly. If you installed Symantec Endpoint Protection Manager, you do not enroll the domain in the cloud. When you upgrade to Symantec Endpoint Security, the equivalent setting in the cloud takes precedence over the Symantec Endpoint Protection Manager setting. If there is no equivalent setting, the previous Symantec Endpoint Protection Manager setting takes precedence.</p> <p>If you upgrade from Symantec Endpoint Protection Manager to the cloud, you can later revert back to managing with Symantec Endpoint Protection Manager. However, you must reinstall the management server if you uninstalled it. Make sure you make a backup of the database before you upgrade in case you need to perform disaster recovery later. You can use the smc command to convert Windows devices back to management by the Symantec Endpoint Protection Manager.</p> <p><a href="#">Upgrading to Symantec Endpoint Security from Symantec Endpoint Protection</a></p> <p><a href="#">Getting started with Endpoint Security</a></p> <p><a href="#">Disaster recovery best practices for Endpoint Protection</a></p>
Manage clients entirely using the on-premises Symantec Endpoint Protection Manager	<p><b>Symantec Endpoint Protection or Symantec Endpoint Security (Enterprise or Complete)</b></p> <p>You do not enroll a SEPM domain in the cloud. You create and deploy the client installation package from the Symantec Endpoint Protection Manager.</p> <p>Use this approach in the following situations:</p> <ul style="list-style-type: none"> <li>• Your network includes remote locations, such as an oil rig or an offshore environment</li> <li>• You work in a government environment where the network is very restricted.</li> <li>• You have a lot of clients in a dark network.</li> <li>• You want the same features as an on-premises management server. However, Symantec Endpoint Protection continues to add features.</li> </ul>

If you want to...	Use this product
Manage both legacy clients and cloud-only managed agents (hybrid)	<p><b>Symantec Endpoint Protection or Symantec Endpoint Security (Enterprise or Complete)</b></p> <p>For a successful hybrid deployment, SEPM and the agents must be version 14.1 or later. You manage the agents and some policies from Symantec Endpoint Security. You manage clients earlier than 14.1 from the Symantec Endpoint Protection Manager.</p> <p>Note: The Symantec Endpoint Protection client is the same as the Symantec Agent.</p> <p>Use this approach in the following situations:</p> <ul style="list-style-type: none"> <li>• You want to upgrade from 14.1 or later to Symantec Endpoint Security but you want to move slowly to a completely cloud-managed console.</li> <li>• You have clients on devices that use operating systems that the Symantec Endpoint Security does not support.</li> <li>• You want to use Application Control, which replaces the Application Control policy in Symantec Endpoint Protection Manager. Application Control requires a 14.2 MP1 or later client. Application Isolation (new) requires the 14.2 RU1 (cloud only) or 14.2 RU1 client or later and uses the Symantec Endpoint Security cloud console.</li> </ul> <p>You must buy the Symantec Endpoint Security Complete subscription for Application Control and Application Isolation.</p> <p>If you upgrade to the hybrid model, and later want to revert back to Symantec Endpoint Protection Manager only, you simply unenroll the Symantec Endpoint Protection Manager domain. This option provides more flexibility; you can move fully to the cloud at a later point.</p> <p><a href="#">Enrolling a Symantec Endpoint Protection Manager domain into the cloud console</a>  <a href="#">Unenrolling Symantec Endpoint Protection Manager domains from the cloud console</a></p>

#### NOTE

The client functions slightly differently if the Symantec Endpoint Protection Manager manages it rather than Symantec Endpoint Security manages it. The Symantec Endpoint Protection Manager controls more options on the client, while Symantec Endpoint Security controls fewer options. The Symantec Endpoint Protection Manager provides more options for the user to configure; the cloud-managed client provides fewer options. However, Symantec adds new features in Symantec Endpoint Security in monthly refreshes.

[Comparison between an on-premises Symantec Endpoint Protection 14.x and Symantec Endpoint Security Complete](#)

## Enrolling a Symantec Endpoint Protection Manager domain into the cloud console

You must first enroll a Symantec Endpoint Protection Manager domain before you can view or manage it in the cloud console.

#### NOTE

You can enroll a maximum of 50 Symantec Endpoint Protection Manager domains.

#### Before you start enrollment

Enrollment with the cloud console installs the Symantec Endpoint Protection Manager bridge service, or connector, using an .MSI file.

Your environment must meet the following requirements to support the enrollment of a domain into the ICDm cloud console:

- Paid subscription to Symantec Endpoint Security Complete or Symantec Endpoint Security Enterprise.
- [Symantec Security Cloud account](#)

You can set up this login account when you initiate domain enrollment from Symantec Endpoint Protection Manager. Or you might have an existing account to use for login.

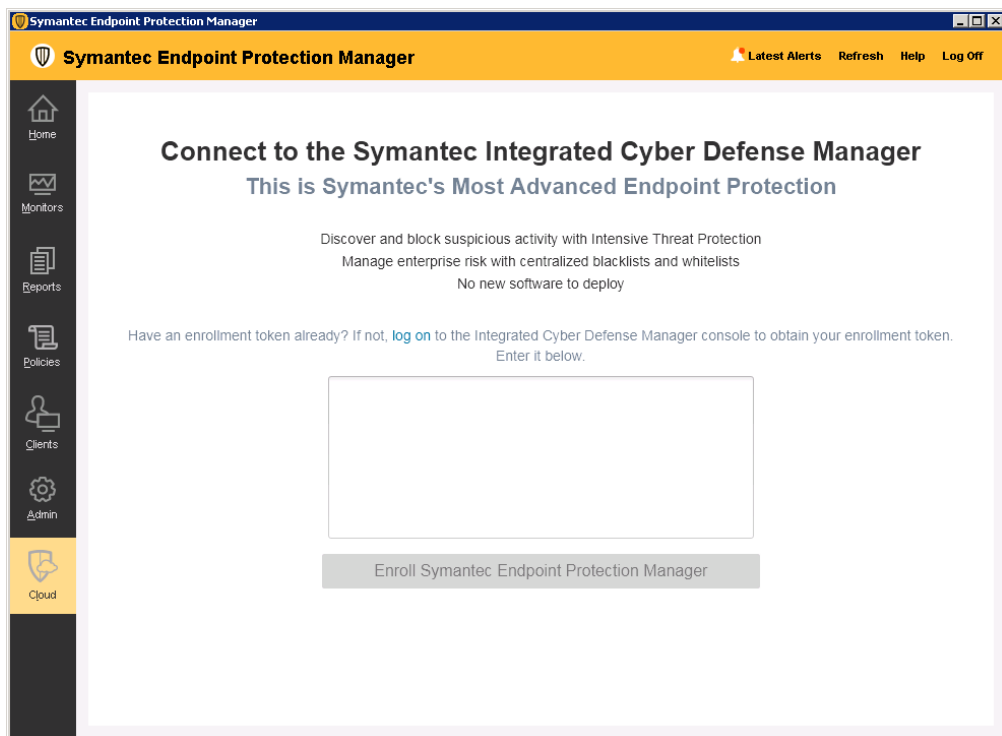
- Administrator access to the Symantec Endpoint Protection Manager
- Symantec Endpoint Protection Manager 14.0.1 or later clients

You can enroll a Symantec Endpoint Protection Manager domain into the cloud console with earlier clients, but these earlier clients cannot take advantage of the cloud-only Intensive Protection policy.

- Put the Application and Device Control into Test (log only) mode and System Lockdown into log-only mode. This situation applies only if such policies apply to the server on which Symantec Endpoint Protection Manager runs, and the policies block .MSI installation.

### Step 1: Start the enrollment

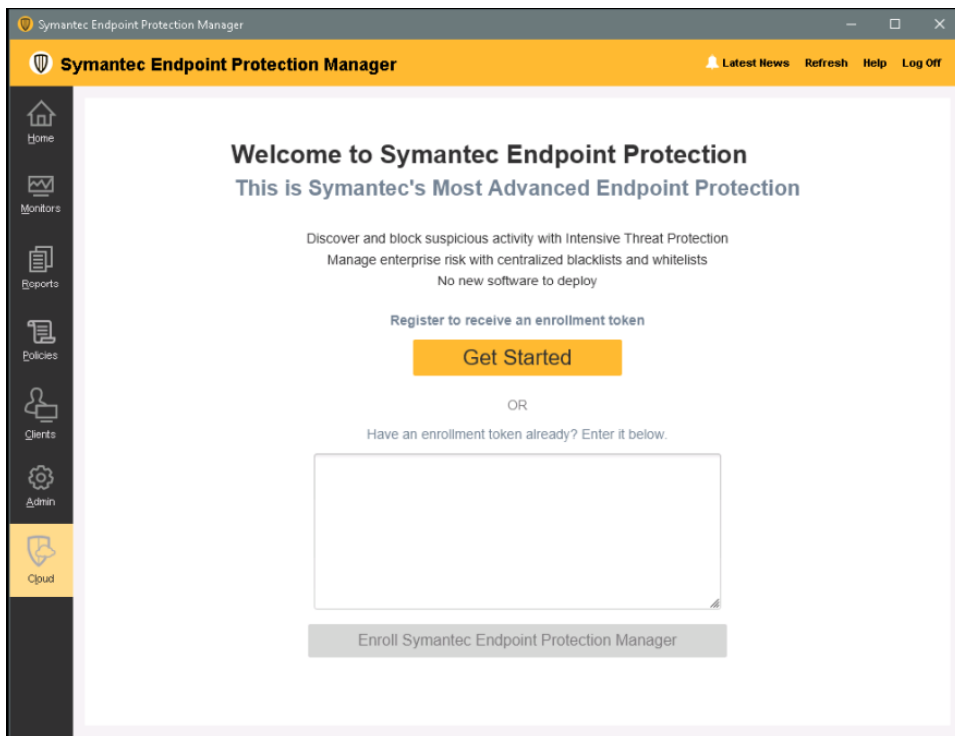
To start the enrollment from Symantec Endpoint Protection Manager 14.3, select the **Cloud** tab.



To start the enrollment from Symantec Endpoint Protection Manager 14.2 or earlier:

In Symantec Endpoint Protection Manager, on the **Home** page select **Enroll Now** or go to the **Cloud** tab. The **Get Started** button takes you to the cloud console sign in page. If you do not have sign in credentials, contact your account team manager.





You can also start the enrollment process from the cloud console on the **Enrollment** page.

## Step 2: Get an enrollment token from the cloud console

In the cloud console, go to **Endpoint > Integration > Enrollment**. You can generate and copy an enrollment token from this page.

## Step 3: Complete the enrollment

1. In Symantec Endpoint Protection Manager, paste the enrollment token into the specified area in the **Cloud** page.
2. Select **Enroll Symantec Endpoint Protection Manager**.  
You get a confirmation message.
3. You can press **Launch** in the Symantec Endpoint Protection Manager **Home** page banner to log on to the cloud console.
4. After enrollment, all of your devices appear in the cloud console. Devices are the client computers that your clients run on. By default, the Symantec Endpoint Protection Manager manages the topology.
5. To manage groups and devices from the cloud console, turn on **Manage Devices from the Cloud** only for the logged-on domain. To manage cloud-based policies, turn on **Manage Policies from the Cloud**. You enable these options in the cloud console in **Endpoint > Integration > Enrollment**.  
You should keep **Manage Devices from the Cloud** disabled if you use Active Directory or third-party APIs to manage your devices.

### WARNING

Whenever you make a change to the device group structure, there is a 10-minute delay before the change appears in Symantec Endpoint Protection Manager. The reverse is also true. The behavior is similar to how Symantec Endpoint Protection Manager replication functions. During the delay, you should not try to make additional topology changes. The changes might not take effect.

[What happens after you enroll a Symantec Endpoint Protection Manager domain into the cloud console?](#)

[Unenrolling Symantec Endpoint Protection Manager domains](#)

---

## What happens after you enroll a Symantec Endpoint Protection Manager domain into the cloud console?

After Symantec Endpoint Protection Manager (SEPM) domain enrollment, Symantec Endpoint Protection Manager data gets synched to the cloud console. The data includes the client hierarchy and the policies that the cloud console supports. The sync time is not immediate. You might have to wait a period of time before you see devices in the cloud console.

Once the devices and policies are synched, you can manage them from either the Symantec Endpoint Protection Manager or the Integrated Cyber Defense Manager cloud console. This is called hybrid management.

Symantec Endpoint Protection Manager client computers and client groups appear on the cloud console automatically as devices on the **Devices** page. By default, the devices appear in a flat list and not in groups on the **Devices** page.

Symantec Endpoint Protection Manager clients are called Symantec Agents in the cloud console.

### Step 1: View the devices that the Symantec Endpoint Protection Manager manages

1. In the cloud console, go to **Endpoint > Devices**.
2. On the **Devices** tab, in the **Managed by** drop-down menu, select **Endpoint Protection Manager**

By default, you manage the organization of your devices in the Symantec Endpoint Protection Manager. You can manage devices in the cloud console only or in Symantec Endpoint Protection Manager only but not both at the same time.

### Step 2: Choose whether to manage devices and groups from the cloud console

1. In the cloud console, go to **Endpoint > Integration**.
2. On the **Enrollment** tab, make sure **Manage Devices from the Cloud** is turned on.

#### NOTE

If you want Active Directory or some other third-party directory tool to manage your device organization, keep this setting turned off.

#### NOTE

Whenever you make a change to the device group structure, there is a 10-minute delay before the change appears in Symantec Endpoint Protection Manager. The reverse is also true. The behavior is similar to how Symantec Endpoint Protection Manager replication functions. During the delay, you should not try to make additional topology changes. The changes might not take effect.

### Step 3: Choose whether to manage policies in the cloud only or Symantec Endpoint Protection Manager only

Policies appear in the cloud console automatically on the **Endpoint > Policies** page. You do not need to export your policies from Symantec Endpoint Protection Manager and import them in the cloud, unless you are going to manage your environment completely from ICDm.

After domain enrollment, the cloud console always controls the supported policies, which you manage from ICDm.

You continue to use Symantec Endpoint Protection Manager to manage other policies, such as the Host Integrity policies. Policies are pushed down to Symantec Endpoint Protection Manager, which distributes them to the clients.

#### To manage policies from the cloud console:

- In the cloud console, go to the **Integration > Enrollment** tab, and turn on **Manage Policies from the Cloud**.

### Step 4: Look for threats that the cloud console detected

The cloud console's **Dashboard** and the **Discovered Items** lists provide more comprehensive information about the detections in your environment. Use the dashboard to check the results of the policy settings and tune the policy settings if necessary.

- In the cloud console, go to **Dashboard > SEP 14.2**.

## How a hybrid-managed Symantec Endpoint Protection Manager interacts with the Symantec Endpoint Security cloud console

This section lists some expected behaviors that may occur when you enroll a Symantec Endpoint Protection Manager domain in the cloud console.

- [Communication and enrollment between the cloud portal and Symantec Endpoint Protection Manager](#)
- [Licensing, installation, upgrading, databases](#)
- Domains enrollment and unenrollment
- [Sites, replication](#)
- [Groups, clients, locations](#)
- [Policies and inheritance](#)

### Communication and enrollment between the cloud console and Symantec Endpoint Protection Manager

- If the Symantec Endpoint Protection Manager connector cannot obtain the access token to the cloud console, it retries every hour.
- Clients that connect through Symantec Endpoint Protection Manager may not immediately display the correct online status in the cloud console. Allow for 5-10 minutes after the online status changes to see an accurate reflection of the current status.

#### [Checking whether the client is connected to the management server and is protected](#)

- The system time for the management server and the Google Cloud Platform (GCP) server must be within 10 minutes of each other. Otherwise, enrollment fails, and you see the following error message:

Enrollment in the cloud console cannot complete because the Symantec Endpoint Protection Manager computer date and time does not match the current date and time. Change the setting in the Control Panel, and then retry the enrollment.

To resolve the time mismatch, synchronize the Symantec Endpoint Protection Manager server with Network Time Protocol (NTP). See the following for more information: [NTP: The Network Time Protocol](#)

- You can use the following logs to troubleshoot a failed enrollment: `BRIDGE_INSTALL.log`, `catalinaWs.out`, `Cloud-0.log`, `scm-server-0.log`, and `semapisrv_access_log.date.log`. All of these files are in `\tomcat\logs`, within the Symantec Endpoint Protection Manager installation folder.

### [Enrolling a Symantec Endpoint Protection Manager domain \(14.1 or later\) into the cloud console](#)

#### [Configuring a management server list for load balancing](#)

### Licensing, installation, upgrading, databases

- You must purchase a Symantec Endpoint Security license to use or enroll in the cloud console.
- You cannot upgrade a management server from the cloud console.
- You cannot back up or restore the database or Symantec Endpoint Protection Manager settings from the cloud.
- To free up licenses, the Symantec Endpoint Protection Manager database deletes the clients that have not connected to the domain, based on the number of days that you specify. In the cloud console, these clients are automatically deleted after 30 days, and you cannot configure this interval. The clients are deleted first in the Symantec Endpoint Protection Manager database and then in the cloud console. [Purging obsolete clients from the database to make more licenses available](#)

### Domain enrollment and unenrollment

When the domain is enrolled:

- Events, policies, clients, and client groups are synchronized.
- Cloud-supported policy features are not available for configuration in Symantec Endpoint Protection Manager.
- Cloud policy settings take precedence.

You can unenroll the default domain if necessary. For example, you might have connectivity issues, or you might decide that you do not want the cloud console to manage your policies. You can unenroll on the enrollment page in Symantec Endpoint Protection Manager or in **Endpoint > Integration > Enrollment** in the cloud console.

The unenrollment process removes the client groups and clients of the unenrolled domain in the cloud. Any associated policies remain in the cloud console as well as related events.

## Unenrolling Symantec Endpoint Protection Manager domains

### Sites, replication

- For each site, you enroll one Symantec Endpoint Protection Manager domain per site in the cloud console. You cannot enroll multiple domains even if the domains are in separate sites. You also cannot enroll separate Symantec Endpoint Protection Manager domains if you use the same cloud console account.
- For sites with two Symantec Endpoint Protection Managers that share a SQL Server database and that are configured for failover, you enroll one domain from one of the management servers. The bridge service that communicates between each management server and the cloud console runs on one management server at a time. The service runs on the management server with the higher server priority first. If the first bridge service goes down, the service to the second management server runs instead. You can only manage one domain at a time from the cloud console. The sync between the cloud console and each management server does occur simultaneously.

[Site configurations that the cloud console supports](#) displays which site configurations the cloud console supports when you enroll a Symantec Endpoint Protection Manager domain.

**Table 174: Site configurations that the cloud console supports**

Site configuration	Supported on the cloud console
One site, one Symantec Endpoint Protection Manager on one computer with a database on the same computer only	Yes
One site, one Symantec Endpoint Protection Manager on one computer with a Microsoft SQL Server database on the second computer	Yes
One site, multiple Symantec Endpoint Protection Managers	Yes
Multiple sites, one Symantec Endpoint Protection Manager on each site, with replication*	Yes (14.2 and later)
Multiple sites, multiple Symantec Endpoint Protection Managers on each site, with replication*	Yes (14.2 and later)

\* Only one Symantec Endpoint Protection Manager on one of the sites in a replication partnership is supported to enroll with the cloud.

## Enrolling sites with replication partners in the cloud console

### Groups, clients, locations

- 
- If you rename **My Company** in the cloud console, the group name does not change in Symantec Endpoint Protection Manager.
  - Cloud-managed features require a managed client. You cannot manage an unmanaged client or apply a policy that uses cloud features to an unmanaged client. If you apply policies that use cloud features to an unmanaged client, the policy defaults to the equivalent legacy Symantec Endpoint Protection options.
  - Version 14, 14 MP1, 14 MP2, and legacy 12.1.x client computers appear in the cloud console, but do not support any of the new cloud-based features.
  - If the **Manage Devices from the Cloud** option is turned on in the cloud console, the cloud console manages the devices. If it is off, then Symantec Endpoint Protection Manager manages the devices.  
If you use Active Directory with Symantec Endpoint Protection Manager to manage groups and clients, then Symantec Endpoint Protection Manager automatically manages devices. In this case, you cannot switch **Manage Devices from the Cloud** to the cloud console. This setting returns control of the device organization only to Symantec Endpoint Protection Manager. It does not affect policy protection on any group. You continue to manage advanced policy features from the cloud console.
  - Whenever you make a change to the device group structure, there is a 10-minute delay before the change appears in Symantec Endpoint Protection Manager. The reverse is also true. The behavior is similar to how Symantec Endpoint Protection Manager replication functions. During the delay, you should not try to make additional topology changes.
  - If you add a group or policy in the cloud console that contains any of the following special characters: `/ \ * ? < > | : " ,`, these characters are converted to a dash in the Symantec Endpoint Protection Manager. For example, if you name a group `Europe***`, on Symantec Endpoint Protection Manager, this group is labeled as `Europe---`.
  - The cloud console supports location awareness for 14.3 and later agents. For earlier agent versions, if a Symantec Endpoint Protection Manager group has multiple locations and each location uses a different policy (shared or non-shared), then only the default location's policy gets synched up and applied to the equivalent group on the cloud console. After the cloud console syncs back with Symantec Endpoint Protection Manager, that group's policy in the cloud console is applied as a shared policy to all the locations in the equivalent group on the Symantec Endpoint Protection Manager. This process applies to both the Memory Exploit Mitigation policy and the Exceptions policy in the Symantec Endpoint Protection Manager.
  - The cloud console does not support a connection over IPv6. Enrollment of Symantec Endpoint Protection Manager over an IPv6 network results in the following error:

An error has occurred requesting the status for this enrollment token.

Symantec Endpoint Protection Manager cannot connect to the cloud console. Check the network connection and try again.



## Policies

- You can manage policy settings for 14.0.1 and later clients from the cloud.  
You must still manage policy settings for clients earlier than 14.0.1 directly from Symantec Endpoint Protection Manager. However, there are exceptions. If you apply an Exceptions policy from the cloud, and the client supports the exception type, then the exception applies to the client regardless of version. Memory Exploit Mitigation policies apply to all version 14 clients and later.
- Policies that come from the cloud do not follow the policy inheritance configuration for Symantec Endpoint Protection Manager. Instead, they follow the inheritance rules that are defined in the cloud.
- In the Virus and Spyware Protection policy, a cloud icon appears next to some options when the domain is enrolled in the cloud console. If an Intensive Protection policy is in effect, the policy overrides these options for 14.0.1 and later clients.
- The first default cloud policies that you create and assign in the cloud console is appended with a `v` and a number (`#`) in Symantec Endpoint Protection Manager, as follows: `Default MEM Policy v1`. If you then unenroll and then reenroll the Symantec Endpoint Protection Manager domain, an additional `v#` is appended to the policy name. For example, `Default MEM Policy v1` may become `Default MEM Policy v1 v1` or `Default MEM Policy v1 v3`. For differences between the Symantec Endpoint Protection Manager Exceptions policy and the cloud console Allow List and Deny List policies:

### [How does the Symantec Endpoint Protection Manager Exceptions policy interact with the cloud console?](#)

- In Symantec Endpoint Protection Manager, some cloud policies appear in the list on the **Clients > Policies** tab. A cloud icon indicates that the policy originates from the cloud.

**Table 175: Cloud icons**

Icon	Description
	The group does not inherit the policy from its parent in the cloud console. The policy applies directly to the group.
	The group inherits the policy from its parent in the cloud console.

Some cloud console policies are new policies and some are cloud versions of existing policies. The client version determines which policies the client supports. If you apply a policy to a client that does not support the policy, the client ignores the policy. This behavior is true whether the policy originates in the cloud console or in Symantec Endpoint Protection Manager. The user interface in Symantec Endpoint Protection Manager indicates which options or entire policies the cloud console controls.

- The hybrid-managed cloud console currently supports Symantec Endpoint Protection Manager policies for Windows clients but not for Mac or Linux clients. You must still manage Mac and Linux clients entirely from the cloud or entirely from Symantec Endpoint Protection Manager.

[How 14.x Symantec Endpoint Protection Manager domain-enrolled cloud console features compare to on-premises Symantec Endpoint Protection Manager](#)

### Policy inheritance

In the cloud console, child device groups inherit policies from their parent device group. However, you can apply policies directly to child groups or child devices. You do not have to turn off inheritance.

[How 14.x Symantec Endpoint Protection Manager domain-enrolled cloud console features compare to on-premises Symantec Endpoint Security](#)

## How 14.x Symantec Endpoint Protection Manager domain-enrolled cloud console features compare to on-premises Symantec Endpoint Protection Manager

You manage policies in both the cloud console and the Symantec Endpoint Protection Manager (SEPM) when your Symantec Endpoint Protection Manager domain is enrolled.

**Table 176: Feature reference**

Symantec Endpoint Protection Manager	Symantec Endpoint Security
<b>Welcome</b> page	<b>Home</b> page The cloud console provides a guided first-time user experience to get you familiar with cloud console features
<b>Home</b> page	<b>Dashboard</b> page The console dashboard shows detailed visibility into suspicious file detections. The dashboard includes a Key Performance Indicator (KPI) bar as well as interactive widgets (charts) with drill-down detail.

Symantec Endpoint Protection Manager	Symantec Endpoint Security
<b>Clients, client groups</b> When the device master option ( <b>Manage Devices from the Cloud</b> ) for the domain is enabled, you must use the cloud console to organize clients and client groups. If you use the Symantec Endpoint Protection Manager, Active Directory, or you use third-party APIs to manage your devices, you should disable this option.	<b>Devices, device groups</b> Managed from the Symantec Endpoint Protection Manager by default. To manage these policies from the cloud, select the <b>Endpoint &gt; Integration &gt; Enrollment &gt; Manage Devices from the Cloud</b> option. This option affects group creation or deletion and device move or deletion only. The feature works similarly to how Active Directory works with Symantec Endpoint Protection Manager. You can view your devices and device groups in the cloud console. You cannot create a group in Symantec Endpoint Protection Manager when its domain is enrolled in the cloud and the device master option is enabled. When the device master option is enabled, the group structure is managed in the cloud.
No corresponding configuration.	<b>Policy group</b>
<b>Policy inheritance</b> In Symantec Endpoint Protection Manager, you must disable policy inheritance if you want to directly apply a policy to a child group. Note: If you unenroll the domain, any MEM policies that you directly applied to child groups from the cloud console are applied to the child groups and their locations regardless of Symantec Endpoint Protection Manager inheritance settings.	<b>Policy inheritance</b> In the cloud console, policy inheritance is always enabled. However, you can always directly apply policies to child groups to override the parent policy.
<b>Monitor and Reports</b> pages	<b>Alerts and Investigate</b> pages You can filter views of alerts and events. Both views provide drill-downs that include enhanced details. A default alert rule notifies the administrator when a specific alert is triggered. Role management provides a way to define which administrators receive alerts about relevant events. You can view and edit predefined alert rules under <b>Alerts &gt; Alert Rules</b> . Event views help you analyze events quickly to make decisions about how to tune policies in your environment. You can view events on the <b>Investigate page</b>
<b>Administrator roles</b> <ul style="list-style-type: none"> <li>System administrator</li> <li>Administrator (domain-based)</li> <li>Limited administrator (policy based)</li> </ul> Cloud console administrators and Symantec Endpoint Protection Manager administrators are not linked in any way.	<b>Administrator roles</b> <ul style="list-style-type: none"> <li>Super Administrator</li> <li>Domain Administrator</li> <li>Limited Administrator</li> <li>Viewer</li> </ul>
<b>Console timeout</b> The default is one hour. You can change the timeout.	<b>Console timeout</b> You cannot change the timeout period. The timeout is 2 hours.
<b>Heartbeat</b> option	Not available. All policy changes happen in real time.

The following table displays which policies are available for a Symantec Endpoint Protection Manager enrolled in the cloud, as well as the minimum client version that supports each policy.

**Note:** Version 14.0.1 and 14.1 are the same version; the 14.01 Windows client was released with a 14.1 Symantec Endpoint Protection Manager.



**Table 177: Policy feature reference**

Symantec Endpoint Protection Manager	Symantec Endpoint Security
<p><b>Out-of-box policies</b>  <b>The following policies continue to be managed in Symantec Endpoint Protection Manager:</b></p> <ul style="list-style-type: none"> <li>• Firewall policy</li> <li>• Device Control</li> <li>• Intrusion Prevention policy</li> <li>• LiveUpdate policy</li> <li>• Host Integrity policy</li> <li>• Virus and Spyware Protection policy options other than Bloodhound, SONAR heuristics, Download Insight, and scan actions.</li> <li>• Application and Device Control</li> <li>• System Lockdown</li> </ul>	<p>Managed from the Symantec Endpoint Protection Manager by default.  To manage the following policies from the cloud, select the <b>Endpoint &gt; Integration &gt; Enrollment &gt; Manage Policies from the Cloud</b>:</p> <ul style="list-style-type: none"> <li>• Intensive Protection policy</li> <li>• System policy (low-bandwidth option only)</li> <li>• Allow List policy</li> <li>• Deny List policy</li> <li>• MEM policy</li> </ul> <p>The fully cloud-managed Symantec Endpoint Security manages additional policies that Symantec Endpoint Protection does not manage:  <a href="#">Quick reference for Symantec Endpoint Protection-managed versus Symantec Endpoint Security-managed features in ICDm</a></p>
<p><b>Download Insight, Bloodhound and SONAR settings in Virus and Spyware Protection policy</b>  The following settings are not applicable to Symantec Endpoint Protection 14.1 or later clients when the domain is enrolled in the cloud console:</p> <ul style="list-style-type: none"> <li>• Virus and Spyware Protection policy detection actions</li> <li>• Bloodhound settings</li> <li>• Download Insight sensitivity slider</li> <li>• Download Insight prevalence, first-seen, and intranet options</li> <li>• SONAR heuristic detection, SONAR aggressive mode, and SONAR suspicious behavior settings</li> </ul> <p>These settings are still used for legacy clients and also for 14.1 or later clients and later if you unenroll the domain.</p> <p>Note: The default Intensive Protection blocking level is less aggressive than the most aggressive Bloodhound setting in a Virus and Spyware Protection policy. If your current policies specify Bloodhound at its highest level, you might need to increase the Intensive Protection level.</p>	<p><b>Intensive Protection policy</b> (14.0.1 or later)  Automatically applied to Windows clients after domain enrollment  Replaces some settings in Virus and Spyware Protection policies for Windows clients.  These clients use the Intensive Protection policy to replace certain existing settings in the Virus and Spyware Protection policy:</p> <ul style="list-style-type: none"> <li>• Bloodhound</li> <li>• SONAR heuristics</li> <li>• Download Insight options</li> <li>• Scan actions</li> </ul> <p>However, clients still use their Virus and Spyware Protection policy for other options.</p>
<p><b>Exceptions policy</b>  In Symantec Endpoint Protection Manager, there is a single Exceptions policy, which contains exclusions for many different items as well as exclusions for applications. The cloud console Allow List and Deny List policies appear as separate policies in Symantec Endpoint Protection Manager.  Items from the cloud console appear in the <b>Exceptions policy &gt; Exceptions</b> list.  When the domain is enrolled, you can only create exceptions for the types that are not supported in the cloud console.  <a href="#">How does the Symantec Endpoint Protection Manager Exceptions policy interact with the cloud console?</a></p>	<p><b>Allow List policy</b> (14.0.1 or later)  Any Allow List policy that you create in the cloud appears in Symantec Endpoint Protection Manager even if you unenroll the domain.  The cloud console includes a central list of items that are allowed or blocked so you can view all of these items in one place.  The Allow List policy was renamed from the Whitelist policy. in 14.3 RU1.</p>



Symantec Endpoint Protection Manager	Symantec Endpoint Security
<b>Exceptions policy</b> Deny List policies from the cloud console are not scan exceptions. However, denied items from the cloud console appear in the <b>Exceptions</b> list.	<b>Deny List policy (14.0.1 or later)</b> Any Deny List policy that you create the cloud appears in Symantec Endpoint Protection Manager even if you unenroll the domain. You can configure exceptions in Symantec Endpoint Protection Manager or in the cloud console. The cloud console currently does not support the full range of exceptions.  <b>Note:</b> The Deny List policy is a type of application control that uses the SONAR technology in Symantec Endpoint Protection Manager to enforce its rules. It does not use the application control driver in Symantec Endpoint Protection Manager.  The Deny List policy was renamed from the Blacklist policy. in 14.3 RU1.
No corresponding option. Symantec Endpoint Protection Manager shows low-bandwidth status. You can see whether or not the low-bandwidth option is enabled in <b>External Communications &gt; Cloud Settings</b> . Symantec Endpoint Protection Manager also manages the LiveUpdate AML content that is required for low bandwidth to work.	<b>System policy (low-bandwidth option) (14.0.1 or later)</b> The System policy is a new policy in the cloud with no corresponding configuration in Symantec Endpoint Protection Manager. However, the low-bandwidth option requires low-bandwidth Advanced Machine Learning (AML) LiveUpdate content to be available on Symantec Endpoint Protection Manager for the policy to work. Default is off.
<b>Memory Exploit Mitigation (MEM) policy</b> When your domain is enrolled, you must use the cloud console to configure this policy.	<b>Exploit Mitigation policy (MEM) policy</b> <ul style="list-style-type: none"> <li>14.0 or later for overall policy features.</li> <li>14.0.1 or later for per-technique configuration.</li> <li>14.2 RU1 for custom applications. You must have Application Isolation enabled. The client must have Application Hardening installed.</li> </ul> The policy options are comparable to the options in Symantec Endpoint Protection Manager.

## How does the Symantec Endpoint Protection Manager Exceptions policy interact with the cloud console?

### How do Exceptions policies work on the cloud console?

The cloud console does not support all the exceptions that the Symantec Endpoint Protection Manager supports. After you enroll a Symantec Endpoint Protection Manager domain in the cloud console, the original Symantec Endpoint Protection Manager Exceptions policy divides into two policy types in the cloud console, based on the types of exceptions. These cloud-based policies are called the Deny List policy and the Allow List policy. The exceptions that the cloud policies do not support remain in the Symantec Endpoint Protection Manager Exceptions policy. After the cloud console and Symantec Endpoint Protection Manager synchronize, the cloud-based policies are imported back into Symantec Endpoint Protection Manager.

For example, assume that in Symantec Endpoint Protection Manager you create a policy that is called SEPM Exceptions Policy. This policy includes an Application exception, a Trusted Web Domain exception, and an Application to Monitor exception. After you enroll in the cloud console, the cloud-based exceptions in SEPM Exceptions Policy are separated into two policies. These policies are called Imported SEPM Exceptions Policy (BL) and Imported SEPM Exceptions Policy (WL). The Deny List policy is created with the Application exception only, and the Allow List policy is created with the Application exception and the Domain exception. The original Symantec Endpoint Protection Manager SEPM Exceptions Policy retains the Application to Monitor exception. After the cloud console synchronizes with Symantec Endpoint Protection Manager, the Symantec Endpoint Protection Manager displays three policies that are assigned to the same group: SEPM Exceptions Policy, Imported SEPM Exceptions Policy (DL) v1, and Imported SEPM Exceptions Policy (AL) v1

---

In the cloud console, the Blacklist policy was renamed to the Allow List policy. The Whitelist policy was renamed to the Allow List policy.

### Creating exceptions for Virus and Spyware scans

In addition, the cloud console's Allow List and Deny List policies do not support all the actions that the Symantec Endpoint Protection Manager Exceptions policy supports. The Application exception in the cloud console's Allow List policy only supports the **Ignore** action. The Application exception in the cloud console's Deny List policy only supports the **Quarantine** action. If you add an Application exception in the Symantec Endpoint Protection Manager Exceptions policy and then enroll Symantec Endpoint Protection Manager in the cloud console, the actions automatically change in the cloud console's policies. The **Log only** action is converted to the **Ignore** action for the Allow List policy. The **Terminate** and **Remove** actions are converted to the **Quarantine** action. After these policies are imported back into Symantec Endpoint Protection Manager, the management server keeps the action from the cloud console policies.

### Monitoring an application to create an exception for the application on Windows clients

#### Which exceptions are supported and not supported on the cloud console?

The cloud console supports the following exceptions on Windows clients:

##### Deny List policy:

- Hash (SHA-256)

##### Allow List policy:

- Certificate
- Filename
- Domain
- Hash
- File path
- Extension
- IPS Host

After you enroll Symantec Endpoint Protection Manager in the cloud console, the Windows exceptions in the Symantec Endpoint Protection Manager Exceptions policy convert to the following policy type and exception type:

**Table 178: Windows exceptions and how they convert to cloud console exceptions**

Symantec Endpoint Protection Manager Exceptions policy	Deny List policy	Allow List policy
Application	Hash (SHA-256 only)	Hash (SHA-256 only)
Certificate	N/A	Certificate
File > Security Risk/SONAR	N/A	Filename
Folder > Security Risk/SONAR	N/A	Path
Trusted Web Domain	N/A	Domain

The following Windows exceptions remain in the Symantec Endpoint Protection Manager Exceptions policy and are not supported in the cloud console:

- 
- Application to Monitor
  - Extensions
  - File - Application Control
  - Folder - Application control
  - Known Risks
  - Tamper Protection Exception
  - DNS or Host File Change Exception

The cloud console does not support Linux client exceptions or Mac client exceptions. All Linux exceptions items and Mac exceptions items remain in the Symantec Endpoint Protection Manager Exceptions policy.

#### **NOTE**

You can also add exceptions directly into the cloud console using a .csv file of checksums that you export from Symantec Endpoint Protection Manager. This file fingerprint list contains the path and the file name and corresponding checksum for each executable file or DLL that resides in a specified path on the computer. See: [Creating a file fingerprint list with checksum.exe](#)

#### [Which Windows exceptions do I use for what type of scan?](#)

#### **Exceptions that users can add on the Windows client**

The Symantec Endpoint Protection Manager Exceptions policy allows you to enable users on the Windows clients to add exceptions (called client restrictions).

If Symantec Endpoint Protection Manager is enrolled in the cloud console, Symantec Endpoint Protection Manager does not display the following client restrictions:

- Application Exception
- File Exception
- Folder Exceptions > Security risk Exception/SONAR Exception
- Trusted Web Domain Exception
- Certificate Exception

#### **NOTE**

In addition, on Windows clients that a cloud-based exceptions policy controls, these exceptions do not appear in the client user interface.

Symantec Endpoint Protection Manager does display the following client restrictions, whether or not Symantec Endpoint Protection Manager is enrolled.

- DNS or Host File Change Exception
- Extension Exception
- Known Risks Exception

#### [Restricting the types of exceptions that users can configure on client computers](#)

#### **Issues with enrolling and synchronizing Exceptions policies with the cloud console**

- A Deny List policy or Allow List policy gets automatically created in the cloud console only if the original Symantec Endpoint Protection Manager Exceptions policy includes the exceptions that the Deny List policy and the Allow List policy support. Otherwise, the cloud console ignores the Exceptions policy.
- After enrollment, only assigned Symantec Endpoint Protection Manager Exceptions policies synchronize with the cloud console and then get imported back onto Symantec Endpoint Protection Manager. Unassigned policies remain in Symantec Endpoint Protection Manager as non-cloud-based Exceptions policies. Also, if the assigned

- Symantec Endpoint Protection Manager Exception policy has no Deny List exceptions or Allow List exceptions, then a corresponding empty Deny List policy and/or empty Allow List policy gets created in the cloud console for that group.
- After enrollment, you can create and assign non-cloud-based Exceptions policies in Symantec Endpoint Protection Manager. However, these policies must include Symantec Endpoint Protection Manager-based exceptions only, and not cloud-based exceptions. If you create and assign a cloud-based Deny List policy or Allow List policy, these policies get synchronized and imported into Symantec Endpoint Protection Manager.
  - Exceptions policies that you created in the cloud console remain in Symantec Endpoint Protection Manager after you unenroll the domain. But these cloud-based policies get unassigned from a group in Symantec Endpoint Protection Manager. You can merge them, reassign them, or delete them if you no longer need them.
  - If you import a Symantec Endpoint Protection Manager Exceptions policy into the cloud console and that policy has application exceptions, the exceptions are lost after import. You must then manually re-add the application exceptions into the cloud console's Deny List and Allow List policies. The cloud console maintains the other types of exceptions, such as the certificate exception.

## Enrolling sites with replication partners in the cloud console

- [How do you enroll a site in the cloud portal?](#)
- [Removing and restoring replication between the sites that are enrolled in the cloud portal](#)
- [Troubleshooting replication for a site in the cloud portal](#)

### How do you enroll a site in the cloud console?

As of version 14.2, you set up replication between one site that is enrolled in the cloud console, and additional sites that are not. You enroll one site as the master site. All other sites can replicate directly with the master site, or replicate with each other. For example, if Site A is the master site, you enroll Site A into the cloud console. You configure Site B and Site C to replicate with Site A. Or, you can configure Site B to replicate with Site A, and configure Site C to replicate with Site B.

**Table 179: Process for enrolling multiple replicated sites**

Task	Description
Step 1: Replicate the two sites before you enroll in the cloud console.	Replicate all policies, groups, and log events before you enroll the master site to avoid any database conflicts. You can also add a replication partner after you enroll the master site in the cloud. The master site can have multiple partner sites. <a href="#">Replicating data immediately</a> <a href="#">What are sites and how does replication work?</a>
Step 2: Enroll the master site.	Choose and enroll one site as the master site to perform the enrollment and any further actions, such as creating policies. For sites with multiple management servers, you only need to enroll one of the management servers. Any additional management servers are enrolled automatically. You do not enroll the second site, or the partner site, in the cloud console
Step 3: Wait for synchronization to occur.	After the enrolled master site and the cloud console synchronize, the following events occur on the master site: <ul style="list-style-type: none"> <li>• The bridge service is installed on all management servers automatically. However, the bridge service is only active on the management server that you used to enroll in the cloud console.</li> <li>• The master site synchronizes reporting events with the cloud console.</li> <li>• The master site uploads the groups, devices, policies, log events, client packages, and definitions for all clients that are not connected to this site.</li> <li>• The master site receives the policies, logs, and commands from the cloud console and immediately passes the data to the clients that communicate with this site.</li> </ul> <a href="#">What happens after you enroll a Symantec Endpoint Protection Manager domain into the cloud console?</a>

Task	Description
Step 4: Replicate the master site and any partner sites.	<p>Schedule the replication so that both sites have the same enrollment data. After the replication occurs, the following events occur on the partner site:</p> <ul style="list-style-type: none"> <li>The partner site receives the content from the cloud console based on the replication schedule with the master site. The clients that are connected to the partner site then receive this data.</li> <li>The partner site gets the enrollment details from the master site. These details appear on the <b>Cloud</b> page &gt; <b>Troubleshooting</b> page.</li> <li>The partner site's management servers do not install the bridge service. Therefore, the partner site does not synchronize directly with the cloud console.</li> </ul> <p><a href="#">How to install a second site for replication</a></p>
Step 5: (Optional) Switch control of groups and devices to the cloud console.	<p>By default, when you enroll an unreplicated Symantec Endpoint Protection Manager domain, the cloud console manages the client group structure. By default, when you enroll a replicated site, Symantec Endpoint Protection Manager manages the group structure.</p> <ul style="list-style-type: none"> <li>If Symantec Endpoint Protection Manager is the master, you can add groups and policies on the master site, which then gets replicated on the partner site.</li> <li>If you make the cloud console the master, first run replication with the partner site. This replication ensures that groups and policies you added on the partner site sync to the cloud console.</li> </ul> <p>To switch control to the cloud console, enable the <b>Manage Devices</b> option after enrollment in <b>Settings &gt; Symantec Endpoint Protection Manager Enrollment</b> in the cloud console.</p>

You cannot perform failover or load balancing for the replicated partner.

#### [Setting up failover and load balancing](#)

#### **Removing and restoring replication between the sites that are enrolled in the cloud console**

If you remove the partnership between the master site and a partner site, you also remove the relationship with the cloud console.

To restore the partnership with the master site, use the **Add Existing Replication Partner** wizard.

You can also enroll the partner site in the cloud console directly as an individual site. In this case, you must create a different Symantec Cyber Defense Manager account. To restore the partnership with the master site, you must unenroll the partner site. Then, on the master site, reconfigure the partnership with the **Management Server Configuration Wizard**.

#### **NOTE**

As a best practice, keep the partner site as an individual site and do not try to restore the replication with the master site.

#### [Disabling replication and restoring replication before and after an upgrade](#)

#### [Reinstalling or reconfiguring Symantec Endpoint Protection Manager](#)

#### **Troubleshooting replication for a site in the cloud console**

To get information about master site enrollment and replication:

- Look for replication events.  
On the master site, open the **System log > Administrative** log type, and look for the **Replication events** event type.  
[Viewing logs](#)
- Look at the partner site's enrollment status.  
On the partner site, the **Enrollment Status** displays **Enrolled**.  
Other fields such as **Connection Status** display **None**.  
To display the enrollment information, click the **Cloud** page > **Troubleshooting**.

---

## Updating clients in low-bandwidth environments

### What is low-bandwidth mode?

In 14.1 and later, the low-bandwidth mode is an option for those environments that meet at least one of the following criteria:

- Require infrequent virus and spyware, SONAR, and IPS content updates
- Have low connectivity to the cloud

Low-bandwidth clients receive updates infrequently. Symantec updates low-bandwidth content once a week. In low-bandwidth mode, you can use the aggressive mode policy to tune the security on your endpoints even more.

### [How does Symantec Endpoint Protection use advanced machine learning?](#)

You must be enrolled in the cloud console to use the low bandwidth option. Low bandwidth is off by default.

- In the cloud console, enable low-bandwidth mode in the Default System Policy (14).
- Make sure that LiveUpdate downloads low-bandwidth content.

#### [Download low-bandwidth content](#)

- Create a client group that gets low-bandwidth content.

#### [Creating a group for low-bandwidth clients](#)

After you enable the low-bandwidth mode, you can see its status in the **Clients** tab in the **Default** view and the **Protection Technology** view. You can also generate reports based on low-bandwidth content distribution.

### [Running reports on the clients that run in low-bandwidth mode](#)

#### Enable the low-bandwidth mode from the cloud

You enable or disable low-bandwidth mode in the cloud console's System Policy.

1. In the Symantec Endpoint Security console, go to **Endpoint > Policies > Default System Policy (14)**. You must have a trial version or purchased version of the product.
2. Turn on **Run in low Bandwidth Mode**.
3. Click **Save Policy**.

#### Download low-bandwidth content to Symantec Endpoint Protection Manager

Advanced Machine Learning content is downloaded and enabled by default. You can use the following procedures to verify that they are enabled.

#### To download low-bandwidth content to Symantec Endpoint Protection Manager

1. In the Symantec Endpoint Protection Manager console, click **Admin > Local Site > Edit Site Properties**.
2. Click to select the **LiveUpdate** tab, then click **Change Selection** next to **Content Types to Download**.
3. Make sure the box next to **Advanced Machine Learning** is checked.
4. Click **OK > OK** to save the changes.

#### To include low-bandwidth content in LiveUpdate Content Policy

In the Symantec Endpoint Protection Manager console, go to **Policies > LiveUpdate**, and then edit the policy that is assigned to the group that contains the low-bandwidth-enabled clients.

1. Click **LiveUpdate Content**, then double-click **LiveUpdate Content Policy**.
2. Under **Windows Settings**, click **Security Definitions**.
3. In the cloud console, click **Devices**, and then add a child group under **My Company**.
4. Ensure that the **Advanced Machine Learning** box is checked.
5. Click **OK** to save the changes.

---

## Creating a group for low-bandwidth clients

1. In the cloud console, click **Devices**, and then add a child group under **My Company**.  
If you cannot add a child group, enable **Manage Devices** in the cloud console (**Settings > Symantec Endpoint Protection Manager Enrollment**). Otherwise, add the group in Symantec Endpoint Protection Manager. If you use Active Directory synchronization, add the group through Active Directory.
2. Apply the System Policy to this group that you previously configured for Low Bandwidth. On the device group, click **Apply Policy**, add the System Policy, and then click **Submit**.
3. In the Symantec Endpoint Protection Manager console, ensure that the LiveUpdate Content Policy that you previously configured applies to the group you created. Policy inheritance that you enable or disable in Symantec Endpoint Protection Manager applies only to Symantec Endpoint Protection Manager policies, and not to cloud console device policies.  
You may need to allow some time for the group to sync from the cloud console.

## Running reports on the clients that run in low-bandwidth mode

You can run a report to list the clients that receive low-bandwidth content.

1. In the Symantec Endpoint Protection Manager console, click **Reports > Quick Reports**, and then make the following selections:
  - Report type: **Computer Status**
  - Select a report: **Low Bandwidth Content Distribution**
2. Select a time range: **Additional Settings for more options**.
3. Click **Create Report**.

## Unenrolling Symantec Endpoint Protection Manager domains from the cloud console

The unenrollment process removes the client groups and clients of the unenrolled domain in the cloud. Any associated policies remain in the cloud console as well as related events.

After you unenroll a Symantec Endpoint Protection Manager domain from the ICDm cloud console, you are no longer able to:

- Manage devices from the cloud console.
- See files and applications on your devices.
- Apply cloud-specific policies to devices and device groups to protect them.

During the unenrollment process, a notification appears on the cloud console and you are not able to:

- Perform any function that is associated with device management, such as creating groups, deleting groups, or moving devices between groups.
- Perform any function that is associated with policy management, such as applying policies to devices or device groups.
- Enroll a new domain until the current domain is unenrolled.

### NOTE

To unenroll domains, you require the **Endpoint Console Super Administrator** role.

### [Creating an administrator account](#)

After unenrollment, you continue to see alerts, events, and policies in the cloud console.

To unenroll a Symantec Endpoint Protection Manager domain

- 
1. On the Endpoint Security cloud console, go to **Endpoint > Integration**.
  2. On the **Enrollment** tab, check the **Domain Enrollment Status > Enrolled** check box and select **Unenroll**.
  3. Choose an appropriate option:
    - **Unenroll** - Select this option if you only want to unenroll Symantec Endpoint Protection Manager from the cloud console.
    - **Unenroll and remove** - Select this option if you want to unenroll Symantec Endpoint Protection Manager from the cloud console and delete all discovered devices and files information.
  4. Type **Unenroll** in the text box to confirm.
  5. Select **Unenroll Domain**.

#### **NOTE**

Typically unenrollment takes two hours to complete.

[Enrolling a Symantec Endpoint Protection Manager domain \(14.1 or later\) into the cloud console](#)



---

## Using Symantec Endpoint Protection in virtual infrastructures

---

Symantec Endpoint Protection provides the Shared Insight Cache and Virtual Image Exception features for virtual infrastructures, which you can enable to improve performance. You need to perform some additional installation and configuration tasks to enable these features.

**Table 180: Virtual infrastructure features and their use**

Feature and use	Description
Use Shared Insight Cache to skip the scanning of files that are known to be clean.	<p>Shared Insight Cache keeps track of the files that are known to be clean. Shared Insight Cache can reduce the scan load by eliminating the need to rescan those files.</p> <p>You can set up the following types of Shared Insight Cache:</p> <ul style="list-style-type: none"><li>• A network-based Shared Insight Cache Virtual clients that use any kind of virtual infrastructure can use a network-based Shared Insight Cache to reduce scan loads.</li></ul> <p><b>Note:</b> As of 14.0, a vShield-enabled Shared Insight Cache is no longer supported.</p> <p><a href="#">About Shared Insight Cache</a> <a href="#">What do I need to do to use a network-based Shared Insight Cache?</a></p>
Use the Virtual Image Exception tool so that clients can skip the scanning of base image files.	<p>The Virtual Image Exception tool lets you mark base image files as safe so that scans skip those files to reduce scan loads.</p> <p>The Virtual Image Exception tool runs in a virtual environment only.</p> <p><a href="#">About the Virtual Image Exception tool</a></p>
Configure the non-persistent virtual desktop infrastructures feature.	<p>Symantec Endpoint Protection clients have a configuration setting to indicate that they are non-persistent virtual clients. You can configure a separate aging period for the offline GVMs in non-persistent virtual desktop infrastructures. Symantec Endpoint Protection Manager removes non-persistent GVM clients that have been offline longer than the specified time period.</p> <p><a href="#">Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures</a> <a href="#">Purging obsolete non-persistent VDI clients to free up licenses</a></p>

The protection technologies in Symantec Endpoint Protection Manager and Symantec Endpoint Protection typically function the same way in virtual infrastructures as they do in physical infrastructures. You can install, configure, and use Symantec Endpoint Protection Manager and Symantec Endpoint Protection clients in virtual infrastructures in the same way as in physical infrastructures.

### About Shared Insight Cache

Shared Insight Cache use improves performance in virtual infrastructures. Files that Symantec Endpoint Protection clients have determined to be clean are added to the cache. The subsequent scans that use the same virus definitions version can ignore the files that are in the Shared Insight Cache. Shared Insight Cache is used only for scheduled and manual scans.

The network-based Shared Insight Cache runs as a Web service that is independent of the Symantec Endpoint Protection client. Shared Insight Cache uses a voting system. After a client uses the latest content to scan a file and determines that it is clean, the client submits a vote to the cache. If the file is not clean, the client does not submit a vote. When the vote count for a file is greater than or equal to the vote count threshold, then Shared Insight Cache considers the file clean. When another client subsequently needs to scan the same file, that client first queries Shared Insight Cache. If the file is marked clean for their current content, then the client does not scan that file.

---

When a client sends a vote to Shared Insight Cache, the cache checks the version of content that the client used to scan the file. If the client does not have the latest content, Shared Insight Cache ignores the vote. If newer content is available, the newer content becomes the latest known content and Shared Insight sets the vote count back to one.

To keep the cache size manageable, Shared Insight Cache uses a pruning algorithm. The algorithm removes the oldest cache entries, which are those with the oldest timestamp, first. This algorithm ensures that the cache size does not exceed the memory usage threshold.

[What do I need to do to use a network-based Shared Insight Cache?](#)

[Customizing Shared Insight Cache settings](#)

[Using Symantec Endpoint Protection in virtual infrastructures](#)

## About the Virtual Image Exception tool

The Virtual Image Exception tool lets clients bypass the scanning of the base image files for threats. This feature reduces the resource load on disk I/O and on the CPU.

Symantec Endpoint Protection supports the use of Virtual Image Exceptions for both managed clients and unmanaged clients.

### NOTE

Symantec does not support the use of the Virtual Image Exception tool in physical environments.

[Using the Virtual Image Exception tool on a base image](#)

[Using Symantec Endpoint Protection in virtual infrastructures](#)

## What do I need to do to use a network-based Shared Insight Cache?

You can use a network-based Shared Insight Cache to improve scan performance.

**Table 181: Tasks to install and use a network-based Shared Insight Cache**

Step	Task
Step 1: Install Shared Insight Cache.	<a href="#">System requirements for implementing a network-based Shared Insight Cache</a> <a href="#">Installing and uninstalling a network-based Shared Insight Cache</a>
Step 2: In the Virus and Spyware policy in Symantec Endpoint Protection Manager, enable your virtual clients to use Shared Insight Cache	<a href="#">Enabling the use of a network-based Shared Insight Cache</a>

After you have installed a Shared Insight Cache, you can optionally do the following tasks:

- Customize any of the service, cache, or log settings for Shared Insight Cache.  
[Customizing Shared Insight Cache settings](#)
- View related events in the log.  
[Viewing network-based Shared Insight Cache log events](#)
- Use the Windows Performance Manager to monitor its performance.  
[Monitoring network-based Shared Insight Cache performance counters](#)

---

## System requirements for implementing a network-based Shared Insight Cache

The network-based Shared Insight Cache server is designed to run on a standalone physical or virtual machine. Shared Insight Cache should not be installed to a system running other database applications or high-availability server applications, such as Symantec Endpoint Protection Manager or Microsoft SQL Server.

The following table describes the minimum system requirements that a virtual infrastructure needs to run Shared Insight Cache.

**Table 182: Network-based Shared Insight Cache system requirements**

Requirement	Description
Software	<ul style="list-style-type: none"><li>• Windows Server 2003 (12.1 through 12.1.4 only)</li><li>• Windows Server 2008 and later</li><li>• Windows Server 2012 and Windows Server 2012 R2 (as of 12.1.5)</li><li>• Windows Server 2016 (As of 14.2 MP1)</li><li>• Windows Server 2019 (As of 14.2 MP1)</li><li>• .NET Framework 4</li></ul>
CPU	Shared Insight Cache must be installed on a dedicated server or a virtual machine.
Memory	2 GB minimum
Available disk space	100 MB minimum

[About Shared Insight Cache](#)

[Installing and uninstalling a network-based Shared Insight Cache](#)

## Installing and uninstalling a network-based Shared Insight Cache

Before you install the network-based Shared Insight Cache, ensure that you have met all the system requirements and that you are logged on as a Windows administrator. You install and run the Shared Insight Cache on a standalone physical or virtual machine.

### NOTE

You should not use DBCS or high-ASCII characters in the host name of the server on which you install a Shared Insight Cache. You should also refrain from using DBCS or high-ASCII characters in the user name that you use to access it. These characters cause the Shared Insight Cache service to fail to start.

[System requirements for implementing a network-based Shared Insight Cache](#)

To install a network-based Shared Insight Cache

1. On the Symantec Endpoint Protection installation file, navigate to the `Tools/Virtualization/SharedInsightCache` folder.
2. Double-click the following file to launch the installation program:

`SharedInsightCacheInstallation.msi`

### NOTE

You can type the following command instead, to launch the same installation program:

---

```
msiexec /i SharedInsightCacheInstallation.msi
```

3. In the **Shared Insight Cache Setup** wizard pane, click **Next**.
4. Read through the Symantec Software license agreement, check **I accept the terms of the License Agreement**, and then click **Next**.
5. On the **Destination Folder** pane, do one of the following tasks:
  - Click **Next** to accept the default location for Shared Insight Cache.
  - Click **Change**, browse to and select a different destination folder, click **OK**, and then click **Next**.
6. On the **Shared Insight Cache Settings** pane, specify the following Shared Insight Cache settings:

<b>Cache Usage (% of Physical Memory)</b>	The maximum size of the cache. When the cache exceeds this threshold, Shared Insight Cache prunes the cache size.
<b>Listening Port</b>	The port on which the server listens.
<b>Status Listening Port</b>	The port that the server uses to communicate status about the server.

7. Click **Install**.
8. When the installation has completed, click **Finish**.

### [Customizing Shared Insight Cache settings](#)

Uninstalling Shared Insight Cache has the same effect as stopping the Shared Insight Cache service. If you are uncertain as to whether you want to permanently uninstall Shared Insight Cache, you can stop the service instead.

### [About stopping and starting the network-based Shared Insight Cache service](#)

#### **NOTE**

To uninstall the Shared Insight Cache, use the appropriate Windows control panel, such as Add or Remove Programs. You must have Windows administrator rights to uninstall Shared Insight Cache.

If you uninstall Shared Insight Cache, you may also want to disable the Shared Insight Cache in Symantec Endpoint Protection Manager. Disabling Shared Insight Cache prevents the Windows Event log from receiving notifications each time clients cannot contact the cache.

## **Enabling the use of a network-based Shared Insight Cache**

For communication with Symantec Endpoint Protection clients over the network, by default Shared Insight Cache uses no authentication and no SSL. If you change Shared Insight Cache settings to Basic authentication with SSL or Basic authentication with no SSL, you must specify a user name and password that can access Shared Insight Cache.

### [Customizing Shared Insight Cache settings](#)

To enable the use of a network-based Shared Insight Cache

1. In the Symantec Endpoint Protection Manager console, open the appropriate Virus and Spyware Protection policy and click **Miscellaneous**.
2. On the **Shared Insight Cache** tab, check **Shared Insight Cache using Network**.
3. Click **Require SSL** if you enabled SSL authentication in the configuration file.
4. In the **Hostname** box, type the host name of the host on which you installed Shared Insight Cache.
5. In the **Port** box, type the port number of Shared Insight Cache.
6. Optionally, if you configured authentication for Shared Insight Cache:
  - In the **Username** box, type the user name.
  - Optionally, click **Change Password** to change the default password (null) to the password that you created for authentication.  
Leave these fields empty if you do not want to use a password.
7. Click **OK**.

[What do I need to do to use a network-based Shared Insight Cache?](#)

## Customizing Shared Insight Cache settings

After you install Shared Insight Cache, you can customize its settings in the configuration file.

The configuration file is an XML file that follows .NET Framework application configuration standards. Shared Insight Cache does not start if there is an invalid configuration, such as invalid XML, incorrect value types, or missing required values.

For more information, see:

[Configuration Editor Tool \(SvcConfigEditor.exe\)](#)

The following table describes the options that you can configure.

**Table 183: Shared Insight Cache configuration options**

Option and default value	Description and comments
Cache Service Listening Port The default value is 9005.	<p>Port on which the service listens. The listening port is used by clients to submit scan results for files and to make requests to determine if the client should scan a file.</p> <p>If the range for the port is not between 0 - 65535, the service does not start.</p> <p>The service does not start if it cannot listen on the specified port.</p> <pre>&lt;endpoint address="http://localhost:9005/1"</pre> <p>By default, the Shared Insight Cache server listens on all IP addresses. To configure the listening IP addresses for HTTP or HTTPS services, you must use Netsh.exe. The Shared Insight Cache server listens on the IP addresses that you specified in the IP Listen List modified by those tools.</p> <p>Netsh.exe is included with Windows Server 2008.</p> <p>For more information, see: <a href="#">Configuring HTTP and HTTPS</a></p>
Status Service Listening Port The default value is 9006.	<p>Port the server uses to communicate status about the server. The status listening port uses a SOAP-based interface on the port specified in the configuration section. This interface provides a mechanism by which an administrator can query information and status about the Cache Server.</p> <p>The service does not start if the range is not between 0 - 65535.</p> <p>The service does not start if it cannot listen on the specified port.</p>

Option and default value	Description and comments
Vote Count The default value is 1.	Number of the clients that must verify that the file is clean before Shared Insight Cache uses the results. The value must be less than or equal to 15. If the value is greater than 15, the server uses the default value. <code>&lt;cache.configuration vote.count="1" /&gt;</code>
Prune Size The default value is 10.	Percentage of memory usage to remove from the cache when the cache hits the memory usage limit. The value must be between 10 and 100. If the value is not between 10 and 100, the server uses the default value. <b>Note:</b> Symantec recommends that you keep the default prune size. <code>&lt;prune.size="10" /&gt;</code>
Memory Usage The default value is 50.	Percentage of size of the cache before Shared Insight Cache starts pruning the cache. Must be greater than or equal to 10. <code>&lt;mem.usage="50" /&gt;</code>
Log File The default value is <code>install_folder\CacheServer.log</code>	A file for the Shared Insight Cache log. <code>&lt;filevalue="CacheServer.log" /&gt;</code>
Log Level The default value is ERROR.	ALL DEBUG INFO WARN ERROR FATAL OFF A value of OFF indicates that Shared Insight Cache does not log any messages. <code>&lt;level value="ERROR" /&gt;</code> <a href="#">Viewing network-based Shared Insight Cache log events</a>
Log Size The default value is 10000.	Size of the log (in bytes) until Shared Insight Cache rolls the log over. <code>&lt;maximumFileSizevalue="10000" /&gt;</code>
Log Backups The default value is 1.	Number of rolled over logs to keep before the oldest log is deleted. A value of 0 indicates that Shared Insight Cache retains no backups. A negative value indicates that Shared Insight Cache retains an unlimited number of backups. <code>&lt;maxSizeRollBackupsvalue="1" /&gt;</code>

Option and default value	Description and comments
Enable SSL Enable authentication	<p>By default, Shared Insight Cache is set up with no authentication and no SSL. It can be changed to Basic authentication with SSL, no authentication with SSL, or Basic authentication with no SSL.</p> <pre> &lt;webHttpBinding&gt; &lt;bindingname="CacheServerBinding"&gt; &lt;!--     Uncomment the appropriate section to get     the desired security.      If enabling ssl modify the uri to use https.     A cert will also have to be installed and     registered for the ip/port. --&gt; &lt;!-- Basic authentication with SSL.--&gt; &lt;security mode="Transport"&gt; &lt;transport clientCredentialType="Basic"/&gt; &lt;/security--&gt; &lt;!-- No authentication with SSL.--&gt; &lt;security mode="Transport"&gt; &lt;transport clientCredentialType="None"/&gt; &lt;/security--&gt; &lt;!-- Basic authentication with no SSL.--&gt; &lt;security mode="TransportCredentialOnly"&gt; &lt;transport clientCredentialType="Basic"/&gt; &lt;/security--&gt; &lt;!-- No authentication with no SSL. DEFAULT --&gt; &lt;securitymode="None"&gt; &lt;transportclientCredentialType="Basic"/&gt; &lt;/security&gt; &lt;/binding&gt; &lt;/webHttpBinding&gt; </pre> <p><a href="#">Enabling the use of a network-based Shared Insight Cache</a></p>

To customize Shared Insight Cache settings

1. Navigate to and open the following file:

C:\Program Files (x86)\Symantec\Shared Insight Cache  
 \SharedInsightCacheInstallation.exe.config

This file path may vary for legacy installations.

2. Make the modifications as needed.
3. Save your changes and close the file.
4. Restart the Shared Insight Cache service.

You must restart the Shared Insight Cache service for changes to all configuration settings except the log level to take effect.

[About stopping and starting the network-based Shared Insight Cache service](#)

[What do I need to do to use a network-based Shared Insight Cache?](#)

---

## About stopping and starting the network-based Shared Insight Cache service

You may need to stop the Shared Insight Cache service temporarily to troubleshoot an issue. After you have resolved the issue, you can restart the service. You can start and stop the service from the Service Control Manager.

Uninstalling Shared Insight Cache has the same effect as stopping the Shared Insight Cache service. If you are uncertain as to whether you want to permanently uninstall Shared Insight Cache, you can stop the service instead.

You must have Windows administrator rights to stop and start the Shared Insight Cache service.

[Troubleshooting issues with Shared Insight Cache](#)

## Viewing network-based Shared Insight Cache log events

You can view the Shared Insight Cache log file to see any events that Shared Insight Cache creates. The log file is located in the installation folder and is named `CacheServer.log`.

Shared Insight Cache prints logs in the following format:

```
[ ] %thread | %d{MM/dd/yyyyHH:mm:ss} | %level | %logger{2} | %message [-]%newline
```

For example:

```
[ ] 4 | 12/15/2010 10:51:37 | INFO | CacheServerService.Service | Started service [-]
```

Modify the configuration file to specify the log level that you want to use for network-based Shared Insight Cache.

[Network-based Shared Insight Cache log levels](#) describes the levels that you can set.

**Table 184: Network-based Shared Insight Cache log levels**

Log level	Description
OFF	OFF indicates that no incidents are logged.
FATAL	FATAL messages require you to take action. These messages are the errors that cause Shared Insight Cache to stop. For example, a FATAL message may indicate that the server IP address is not available, which means that Shared Insight Cache cannot run.
ERROR	ERROR messages require you to take action, but the process continues to run. They are errors in the system that cause Shared Insight Cache to fail or lose functionality. You also receive all log entries for FATAL messages. This level is the default logging level.
WARN	WARN messages indicate Shared Insight Cache behavior that may be undesirable, but do not cause it to fail. You also receive all log entries for FATAL messages and ERROR messages.
INFO	INFO messages describe the general actions of or give information about Shared Insight Cache. They may indicate the state of the system and help validate behavior or track down issues. However, alone they are not intended to report actionable items. For example, an information message may indicate that cache pruning is complete. The message does not detail a problem. It only logs behavior. You also receive all log entries for FATAL messages, ERROR messages, and WARN messages.
DEBUG ALL	DEBUG and ALL log level messages produce the same results. These log levels are intended for Support to troubleshoot problems with Shared Insight Cache. You also receive all log entries for all other log levels.



---

Increase the log level only when you need to troubleshoot issues with Shared Insight Cache. When you increase the log level, you begin to significantly increase the size of the log file. When you resolve the issue, return to the default log level of ERROR.

Go to the following location:

Installation folder/CacheServer.log

[Customizing Shared Insight Cache settings](#)

## Monitoring network-based Shared Insight Cache performance counters

You can view network-based Shared Insight Cache statistics in the Windows Performance Monitor. The Shared Insight Cache service must be running to view its performance counters.

**Table 185: Shared Insight Cache statistics**

Statistic	Description
The number of items in the cache	This number represents the current number of items in the cache.
The number of items in the cache that have been voted clean	This number represents the current number of items in the cache, which have been voted clean.
Number of cache requests	The number of cache requests that have been made to the Shared Insight Cache service. This number includes only the number of valid requests that received a 200 response. This counter does not persist across restarts of the service.
Number of update requests	The number of update requests that have been made to the service. This number is only the valid requests that received a 200 response. This counter does not persist across restarts of the service.

To monitor network-based Shared Insight Cache performance counters

1. At the command prompt, type the following command:

```
perfmon
```

2. In the **Performance** window, right-click the graph.
3. Select **Add Counters**.
4. In the **Performance object** drop-down list, select **Shared Insight Cache**.
5. Select the counters that you want to view, and click **Add**.
6. Click **Close**.

The Shared Insight Cache counters that you selected appear in the Performance graph.

For more information about using the Windows performance monitor, see your Windows documentation.

[Troubleshooting issues with Shared Insight Cache](#)

[What do I need to do to use a network-based Shared Insight Cache?](#)

## Troubleshooting issues with Shared Insight Cache

[Troubleshooting Shared Insight Cache](#) provides suggestions for how to troubleshoot issues with Shared Insight Cache.

**Table 186: Troubleshooting Shared Insight Cache**

Issue	Explanation/Resolution
Experiencing problems with the cache results	Restart the service. <a href="#">About stopping and starting the network-based Shared Insight Cache service</a>
Shared Insight Cache returns a "no result" response	Shared Insight Cache returns a no result response when it fails to successfully perform a cache lookup. If the client requests a cache lookup, a no result means that the file must be scanned.  <b>Note:</b> Shared Insight Cache returns a success response even when it fails to successfully perform a cache update. The reason is because the client is not required to perform a different action when a failure occurs.
Suspected issues with HTTP traffic	View the HTTP traffic error log. The HTTP traffic errors are logged in the following location: %Windir%\System32\Logfiles\HTTPERR

[Viewing network-based Shared Insight Cache log events](#)

[Monitoring network-based Shared Insight Cache performance counters](#)

## Using the Virtual Image Exception tool on a base image

You can use the Virtual Image Exception tool on a base image before you build out your virtual machines. The Virtual Image Exception tool lets your clients bypass the scanning of base image files for threats, which reduces the resource load on disk I/O. It also improves CPU scanning process performance in your virtual desktop infrastructure.

Symantec Endpoint Protection supports the use of the Virtual Image Exception tool for managed clients and unmanaged clients

### NOTE

You cannot use the Virtual Image Exception tool in a non-virtual environment.

**Table 187: Process for using the Virtual Image Exception tool on a base image**

Step	Action
Step 1	On the base image, perform a full scan all of the files to ensure that the files are clean. If the Symantec Endpoint Protection client quarantines infected files, you must repair or delete the quarantined files to remove them.
Step 2	Ensure that the client's quarantine is empty.
Step 3	Run the Virtual Image Exception tool from the command line to mark the base image files. <a href="#">Running the Virtual Image Exception tool</a> <a href="#">vietool</a>
Step 4	Enable the feature in Symantec Endpoint Protection Manager so that your clients know to look for and bypass the marked files. <a href="#">Configuring Symantec Endpoint Protection to bypass the scanning of base image files</a>
Step 5	Remove the Virtual Image Exception tool from the base image.

The Virtual Image Exception tool supports fixed, local drives. It works with the files that conform to the New Technology File System (NTFS) standard.

[System requirements for the Virtual Image Exception tool](#)

## System requirements for the Virtual Image Exception tool

The Virtual Image Exception tool is supported for use on VMware ESX, Microsoft Hyper-V, and Citrix XenDesktop platforms.

---

**The client must meet all of the following requirements:**

- The client must be installed in one of the supported virtual environments.
- The client must run Symantec Endpoint Protection client software version 12.1 or later.

**WARNING**

The client must be the same version as the Virtual Image Exception tool.

For the most up-to-date information about requirements and supported platforms, see the following webpage:

[Release notes, new fixes, and system requirements for all versions of Endpoint Protection](#)

[Using the Virtual Image Exception tool on a base image](#)

## Running the Virtual Image Exception tool

Before you run the Virtual Image Exception tool, ensure that you have met all of the system requirements.

**WARNING**

The client must be the same version as the Virtual Image Exception tool.

[System requirements for the Virtual Image Exception tool](#)

To run the Virtual Image Exception tool

1. From the Symantec Endpoint Protection Tools folder of the installation file, download the following file to the base image:

```
/Virtualization/VirtualImageException/vietool.exe
```

2. Open a command prompt with administrative privileges.
3. Run the Virtual Image Exception tool with the proper arguments.

For example, type: `vietool c: --generate`

[vietool](#)

## Configuring Symantec Endpoint Protection to bypass the scanning of base image files

After you run the Virtual Image Exception tool on base image files, you can enable the use of Virtual Image Exceptions in Symantec Endpoint Protection Manager. Once the feature is enabled, virtual clients look for the attribute that the tool inserted. Symantec Endpoint Protection then skips the scanning of base image files that contain the attribute.

You can bypass the scanning of unchanged base image files for Auto-Protect scanning or administrator-defined scans (such as manual scans or scheduled scans).

To configure Symantec Endpoint Protection to use Virtual Image Exception to bypass the scanning of base image files

1. On the console, open the appropriate Virus and Spyware Protection policy.
2. Under **Advanced Options**, click **Miscellaneous**.
3. On the **Virtual Images** tab, check the options that you want to enable.
4. Click **OK**.

[Using the Virtual Image Exception tool on a base image](#)

## Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures

Configure Symantec Endpoint Protection in a virtual environment

**Table 188: Tasks to use Symantec Endpoint Protection in non-persistent virtual desktop infrastructures**

Step	Description
Step 1: Set up the base image.	You configure the Symantec Endpoint Protection client in your base image to indicate that it is a non-persistent virtual client. <a href="#">Setting up the base image for non-persistent guest virtual machines in VDIs</a>
Step 2: In Symantec Endpoint Protection Manager, configure a separate purge interval for offline non-persistent VDI clients.	Symantec Endpoint Protection Manager removes the non-persistent GVM clients that have been offline longer than the specified time period. This feature makes it simpler to manage the GVMs in Symantec Endpoint Protection Manager. <a href="#">Purging obsolete non-persistent VDI clients to free up licenses</a>

## Setting up the base image for non-persistent guest virtual machines in VDIs

You can set your base image up to make it simpler to use Symantec Endpoint Protection Manager to manage GVMs in non-persistent virtual desktop infrastructures.

**Table 189: Tasks to set up the base image for non-persistent GVMs**

Step	Description
Step 1: Install Symantec Endpoint Protection on the base image.	<a href="#">Choosing a method to install the client using the Client Deployment Wizard</a>
Step 2: Disable Tamper Protection in the management server so that you can modify the registry.	<a href="#">Changing Tamper Protection settings</a>
Step 3: Make sure that Symantec Endpoint Protection Manager correctly counts the number of licenses for non-persistent virtual clients.	The advantage of non-persistent clients is that offline non-persistent clients do not count toward the number of deployed licenses. Only online clients count. To mark a virtual client as a non-persistent client, you must create a registry key in the base image. <a href="#">How to manage the license count for non-persistent VDI clients</a>
Step 4: In Symantec Endpoint Protection Manager, re-enable Tamper Protection.	<a href="#">Changing Tamper Protection settings</a>

After you have finished setting up the base image, you can configure a separate purge interval for non-persistent clients in Symantec Endpoint Protection Manager.

[Purging obsolete non-persistent VDI clients to free up licenses](#)

---

## Purging obsolete non-persistent VDI clients to free up licenses

Over time, obsolete clients can accumulate in the Symantec Endpoint Protection Manager database. Obsolete clients are those clients that have not connected to Symantec Endpoint Protection Manager for 30 days. Symantec Endpoint Protection Manager purges obsolete clients every 30 days by default.

If you do not want to wait the same number of days to purge obsolete non-persistent clients, you can configure a separate interval for them. If you do not configure a separate interval, then offline non-persistent virtual clients are purged at the same interval that obsolete physical clients are purged.

Online non-persistent clients count toward the number of deployed licenses; offline non-persistent clients do not.

### [How to manage the license count for non-persistent VDI clients](#)

You can also filter the offline non-persistent clients out of the view on the **Clients** page.

To purge obsolete non-persistent VDI clients to free up licenses

1. In the Symantec Endpoint Protection Manager console, on the **Admin** page, click **Domains**.
2. In the **Domains** tree, click the desired domain.
3. Under **Tasks**, click **Edit Domain Properties**.
4. On the **Edit Domain Properties > General** tab, check the **Delete non-persistent VDI clients that have not connected for specified time** check box and change the **days** value to the desired number.

The **Delete clients that have not connected for specified time** option must be checked to access the option for offline non-persistent VDI clients.

5. Click **OK**.

### [Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures](#)

## How to manage the license count for non-persistent VDI clients

The management server counts each license for clients on physical computers, whether the computer is online or offline. For virtual clients, the management server counts the licenses of online non-persistent clients only. Offline non-persistent clients do not count. Make your virtual clients non-persistent if you have more users than you have clients.

To mark a virtual client as a non-persistent client, you must create a registry key in the base image.

To manage the license count for non-persistent VDI clients

1. After you have installed the Symantec Endpoint Protection client and disabled Tamper Protection, open the registry editor on the base image.

### [Changing Tamper Protection settings](#)

2. Navigate to one of the following registry keys:
  - On 32-bit systems: HKEY\_LOCAL\_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\
  - On 64-bit systems: HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\
3. Create a new subkey named `Virtualization`.
4. In the **Virtualization** subkey, create a key of type DWORD named `IsNPVDIClient` and assign it a value of 1.

### [Purging obsolete non-persistent VDI clients to free up licenses](#)

### [Setting up the base image for non-persistent guest virtual machines in VDIs](#)

---

# viertools

## viertools

viertools - Runs the Virtual Image Exception tool

### **SYNOPSIS**

```
viertools.exe volume: --generate|clear|verify|hash [options ...]
```

### **DESCRIPTION**

The `viertools` command marks the base image files on the volume that you specify by adding an attribute.

### **OPTIONS**

#### **--generate**

Runs the Virtual Image Exception tool on all files on the volume specified. You cannot use this option with `--clear`.

For example: `viertools c: --generate`

#### **--verify**

Verifies that the Virtual Image Exception is set on all files on the specified volume. You cannot use this option with `--clear`.

For example: `viertools c: --verify`

#### **--clear**

Removes the Virtual Image Exception on all files on the volume specified.

For example: `viertools.exe c: --clear`

To delete a specific file: `viertools.exe c:\Users\Administrator\target.file --clear`

You can use a fully qualified path in place of the volume identifier to clear the Virtual Image Exception on a single file or the contents of a folder. Only one file name, folder name, or volume identifier per command line is allowed.

You cannot use this command with `--generate`, `--verify`, or `--hash`.

You must restart the client after you run the `--clear` command.

#### **--hash**

Generates the hash value on all files on the volume specified.

The Virtual Image Exception tool uses the hashes to exclude local files from future scans. The clients compute file hashes separately to send to the Shared Insight Cache to store scan results. You cannot use this option with `--clear`.

For example: `viertools.exe c: --generate --hash`

#### **--volume arg**

Specifies the volume the tool scans.

This option can be a file when you use the `--clear` option. You must specify the volume, and it can be specified either with the volume flag or alone. For example, with the flag `viertools.exe --volume c: --generate`, or alone `viertools.exe c: --generate`.

#### **--verbose**

Outputs to the console the maximum amount of program execution information.

#### **--stop**

Stops on the first error that the tool encounters. Otherwise the tool writes error information to the console and continues.

#### **--help**

Displays this help message.

---

# Troubleshooting Symantec Endpoint Protection

---

How to troubleshoot problems with Symantec Endpoint Protection

[Common issues you can troubleshoot](#) displays the most common issues that you might encounter when you install and use Symantec Endpoint Protection.

**Table 190: Common issues you can troubleshoot**

Task	Description
Fixing installation problems	You can download and run the Symantec Diagnostic Tool (SymDiag) to verify that your computers are ready for installation. The tool is provided from the Symantec Support website through Help on the management server and the client. <a href="#">Troubleshooting computer issues with the Symantec Diagnostic Tool (SymDiag)</a> <a href="#">Identifying the point of failure of an installation</a>
Handling virus outbreaks	You can prevent threats from attacking computers on your network. <a href="#">Preventing and handling virus and spyware attacks on client computers</a> <a href="#">Removing viruses and security risks</a> If a threat does attack a client computer, you can identify and respond to the threat. <a href="#">Virus removal and troubleshooting on a network</a>
Troubleshooting content update problems	If the latest virus definitions do not update correctly on Symantec Endpoint Protection Manager or the clients, see the following article: <a href="#">Troubleshoot LiveUpdate and definition issues with Endpoint Protection Manager</a> <a href="#">Symantec Endpoint Protection: LiveUpdate Troubleshooting Flowchart</a>
Fixing communication problems	The communication channels must be open between all of the Symantec Endpoint Protection components. These channels include the following: server to client, server to database, and server and client to the content delivery component, such as LiveUpdate. <a href="#">Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client</a> <a href="#">Troubleshooting communication problems between Symantec Endpoint Protection Manager and the console or the database</a> <a href="#">Best Practices and Troubleshooting for Group Update Providers</a>
Performing disaster recovery	In case of database corruption or hardware failure, you can restore the latest snapshot of the database if you have a database backup file. <a href="#">Disaster recovery best practices for Endpoint Protection</a>
Reducing the space in the database	You can make more space available on the database if the database size gets too large. <a href="#">Maintaining the database</a>
Troubleshooting reporting issues	You can solve various report and log issues. <a href="#">Troubleshooting reporting issues</a>
Troubleshooting replication issues	<a href="#">Replication Troubleshooting Flowchart for Symantec Endpoint Protection</a>

[What are the tools included with Symantec Endpoint Protection?](#)

---

## URLs that allow (whitelist) SEP and SES to connect to Symantec servers

Symantec Endpoint Protection (SEP) and the clients (Symantec Agents) communicate with specific URLs to perform multiple functions, such as validating licenses, submitting samples of suspicious files, and communicating with the on-premises Symantec Endpoint Protection Manager or the cloud console. You must allow these URLs if you use one or more proxies in your environment to redirect the necessary traffic to the Symantec servers.

[URLs that allow SEP and SES to connect to Symantec servers](#)

## Troubleshooting computer issues with the Symantec Diagnostic Tool (SymDiag)

You can download a utility to diagnose common issues you encounter with installing and using Symantec Endpoint Protection Manager or the Symantec Endpoint Protection client.

You can download a utility to diagnose common issues you encounter with installing and using the Symantec Endpoint Protection client.

The support tool helps you with the following issues:

- Lets you quickly and accurately identify known issues.
  - When the tool recognizes an issue, the tool redirects you to the resources to resolve the issue yourself.
  - When an issue is not resolved, the tool lets you easily submit data to Support for further diagnostics.
1. Do one of the following tasks:
    - See: [Download the Symantec Diagnostic Tool \(SymDiag\) to detect Symantec product issues](#)
    - In either the Symantec Endpoint Protection Manager or the client, click **Help > Download Symantec Diagnostic Tool**
  2. Follow the on-screen instructions.

## Identifying the point of failure of a client installation

The Windows Installer and Push Deployment Wizard create log files that can be used to verify whether or not an installation was successful. The log files list the components that were successfully installed and provide a variety of details that are related to the installation package. You can use the log file to help identify the component or the action that caused an installation to fail. If you cannot determine the reason for the failed installation, you should retain the log file. Provide the file to Symantec Technical Support if it is requested.

### NOTE

Each time the installation package is executed, the log file is overwritten.

1. In a text editor, open the log file that the installation generated.
2. To find failures, search for the following entry:

Value 3

The action that occurred before the line that contains this entry is most likely the action that caused the failure. The lines that appear after this entry are the installation components that have been rolled back because the installation was unsuccessful.

[Choosing a method to install the client using the Client Deployment Wizard](#)



# Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client

If you have trouble with client and server communication, you should first check to make sure that there are no network problems. You should also check network connectivity before you call Symantec Technical Support.

You can check the communication between the client and the management server in several ways.

**Table 191: Checking the connection between the management server and the client**

What to check	Solution
Look on the client to see if the client connects to the management server	You can download and view the troubleshooting file on the client to verify the communication settings. <a href="#">Symantec Endpoint Protection client status icons</a> <a href="#">Checking the connection to the management server on the client computer</a> <a href="#">Investigating protection problems using the troubleshooting file on the client</a>
Test the connectivity between the client and the management server	You can perform several tasks to check the connectivity between the client and the management server. <ul style="list-style-type: none"><li>• <a href="#">Enabling and viewing the Access log to check whether the client connects to the management server</a></li><li>• Ping the management server from the client computer. <a href="#">Using the ping command to test the connectivity to the management server</a></li><li>• Use a Web browser on the client computer to connect to the management server. <a href="#">Using a browser to test the connectivity to Symantec Endpoint Protection Manager on the Symantec Endpoint Protection client</a></li></ul>
Check that the management server uses the correct server certificate	If you reinstalled Symantec Endpoint Protection Manager, check that the correct server certificate was applied. If the management server uses a different server certificate, the server still downloads content, but the client cannot read the content. If the management server uses the wrong server certificate, you must update it. <a href="#">Updating or restoring a server certificate</a> <a href="#">Best practices for updating server certificates and maintaining the client-server connection</a> <b>You can verify that the management server uses the wrong server certificate by checking the following items:</b> <ul style="list-style-type: none"><li>• The client does not display the green dot in the taskbar, which indicates that it does not communicate with the management server. <a href="#">Checking whether the client is connected to the management server and is protected</a></li><li>• The client does not receive policy updates from the management server.</li><li>• The management server shows that it does connect with the client. <a href="#">Symantec Endpoint Protection client status icons</a></li></ul>
Check for any network problems	<b>You should verify that there are no network problems by checking the following items:</b> <ul style="list-style-type: none"><li>• Test the connectivity between the client and the management server first. If the client computer cannot ping or Telnet to the management server, you should verify the DNS service for the client.</li><li>• Check the client's routing path.</li><li>• Check that the management server does not have a network problem.</li><li>• Check that the Symantec Endpoint Protection firewall (or any third-party firewall) does not cause any network problems.</li></ul>
Check the debug logs on the client	You can use the debug log on the client to determine if the client has communication problems. <a href="#">Checking the debug log on the client computer</a> <a href="#">Checking the inbox logs on the management server</a>
Recover lost client communication	If the clients have lost the communication with a management server, you can use a tool to recover the communication file. <a href="#">Restoring client-server communication settings by using the SylinkDrop tool</a>

---

If Symantec Endpoint Protection Manager displays logging errors or HTTP error codes, see the following article:  
[Symantec Endpoint Protection Manager Communication Troubleshooting](#).

## Checking the connection to the management server on the client computer

If you have a managed client, you can check your connection to the management server. If you are not connected to the management server, you can request that your client connect.

[Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)

Checking the connection to the management server on the client computer

1. On the **Status** page, click **Help > Troubleshooting**.
2. In the **Troubleshooting** dialog box, click **Connection Status**.
3. In the **Connection Status** pane, you can see the last attempted connection and the last successful connection.
4. To reestablish a connection with the management server, click **Connect Now**.

## Investigating protection problems using the troubleshooting file on the client

To investigate client problems, you can examine the `Troubleshooting.txt` file on the client computer. The `Troubleshooting.txt` file contains information about policies, virus definitions, and other client-related data.

Symantec Technical Support might request that you email the `Troubleshooting.txt` file.

[Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)

To export the troubleshooting file from the client

1. On the client computer, open the client.
2. In the client, click **Help > Troubleshooting**.
3. In the **Management** pane, under **Troubleshooting Data**, click **Export**.
4. In the **Save As** dialog box, accept the default troubleshooting file name or type a new file name, and then click **Save**.

You can save the file on the desktop or in a folder of your choice.

5. Using a text editor, open `Troubleshooting.txt` to examine the contents.

## Enabling and viewing the Access log to check whether the client connects to the management server

You can view the Apache HTTP server Access log on the management server to check whether the client connects to the management server. If the client connects, the client's connection problem is probably not a network issue. Network issues include the firewall blocking access, or networks not connecting to each other.

You must first enable the Apache HTTP server Access log before you can view the log.

### NOTE

Disable the log after you view it because the log uses unnecessary CPU resources and hard disk space.

[Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)

---

## NOTE

The default for SEPM\_Install is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager.

1. To enable the Apache HTTP server Access log, in a text editor, open the file SEPM\_Install\apache\conf\httpd.conf.
2. In the httpd.conf file, remove the hash mark (#) from the following text string and then save the file:  

```
#CustomLog "logs/access.log" combined
```
3. Stop and restart the Symantec Endpoint Protection Manager service and Apache HTTP server:  
[Stopping and starting the management server service](#)  
[Stopping and starting the Apache Web server](#)
4. To view the Apache HTTP server Access log, on the management server, open the file SEPM\_Install\apache\logs\access.log.
5. Look for a client computer's IP address or host name, which indicates that clients connect to the Apache HTTP server.
6. Disable the Apache HTTP server Access log.

## Stopping and starting the Apache Web server

When you install Symantec Endpoint Protection Manager, it installs the Apache Web server. The Apache Web server runs as an automatic service. You may need to stop and restart the Web server to enable the Apache HTTP Server Access log.

### [Enabling and viewing the Access log to check whether the client connects to the management server](#)

1. To stop the Apache Web server, from a command prompt, type:

```
net stop semwebsrv
```

2. To start the Apache Web server, from a command prompt, type:

```
net start semwebsrv
```

## Using the ping command to test the connectivity to the management server

You can try to ping the management server from the client computer to test connectivity.

### [Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)

To use the ping command to test the connectivity to the management server

1. On the client, open a command prompt.
2. Type the ping command. For example:

```
ping name
```

where name is the computer name of the management server. You can use the server IP address in place of the computer name. In either case, the command should return the server's correct IP address.

If the ping command does not return the correct address, verify the DNS service for the client and check its routing path.

## Using a browser to test the connectivity to Symantec Endpoint Protection Manager on the Symantec Endpoint Protection client

You can use a web browser on the client computer to test the connectivity between the management server and the client. This method helps determine whether the problem is with the connection or network, or with the client itself.

---

You can also check the connection between the management server and the client computer by using the following methods:

- Checking whether the Symantec Endpoint Protection client status icon shows a green dot.

[Symantec Endpoint Protection client status icons](#)

- Checking the connection status on the Symantec Endpoint Protection client.

[Checking the connection to the management server on the client computer](#)

To use a browser to test the connectivity to Symantec Endpoint Protection Manager on the Symantec Endpoint Protection client

1. On the client computer, open a web browser, such as Internet Explorer.
2. In the browser command line, type the following command:

```
http://SEPMServer:8014/secars/secars.dll?hello,secars
```

where SEPMServer is the management server's DNS name, NetBIOS name, or IP address.

IP address includes IPv4 and IPv6. You must enclose the IPv6 address with square brackets: `http://[SEPMServer]:port number`

3. When the webpage appears, look for one of the following results:
  - If the word **OK** appears, the client computer connects to the management server. Check the client for a problem.
  - If the word **OK** does not appear, the client computer does not connect to the management server. Check the client's network connections and that network services are running on the client computer. Verify the DNS service for the client and check its routing path.

[Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)

## Checking the debug log on the client computer

You can check the debug log on the client. If the client has communication problems with the management server, status messages about the connection problem appear in the log.

[Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)

**You can check the debug log by using the following methods:**

- In the client, on the Help and Support menu, in the Troubleshooting dialog box, you can click **Edit Debug Log Settings** and type a name for the log. You can then click **View Log**.
- You can use the Windows registry to turn on debugging in the client.

You can find the Windows registry key in the following location:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\smc\_debuglog\_on

## Checking the inbox logs on the management server

You can use a Windows registry key to generate logs about activity in the management server inbox. When you modify the Windows registry key, the management server generates the logs (ersecreg.log and exsecars.log). You can view these logs to troubleshoot client and server communication.

[Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)

[Checking the debug log on the client computer](#)

To check the inbox logs on the management server

- 
1. On the management server, under HKEY\_LOCAL\_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM, set the DebugLevel value to 3.

The inbox appears in the following default location on the management server computer: SEPM\_Install\data\inbox\log

The default for SEPM\_Install is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager.

2. Open the log with Notepad.

## Restoring client-server communication settings by using the SylinkDrop tool

The Sylink.xml file includes communication settings between the client and a Symantec Endpoint Protection Manager server. If the clients have lost the communication with a management server, you must replace the old Sylink.xml file with a new Sylink.xml file. The SylinkDrop tool automatically replaces the Sylink.xml file on the client computer with a new Sylink.xml file.

### NOTE

You can also replace the Sylink.xml file by redeploying a client installation package. Use this method for a large number of computers, for computers that you cannot physically access easily or computers that require administrative access.

[Restoring client-server communications with Communication Update Package Deployment](#)

**When you run the SylinkDrop tool, it can also perform the following tasks:**

- Migrates or moves clients to a new domain or management server.
- Restores the communication breakages to the client that cannot be corrected on the management server.
- Moves a client from one server to another server that is not a replication partner.
- Moves a client from one domain to another.
- Converts an unmanaged client to a managed client.

You can write a script with the tool to modify communication settings for large numbers of clients.

[About managed and unmanaged clients](#)

[Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)

To restore client-server communication settings by using the SylinkDrop tool for Windows

1. In the console, export the communications file from the group that connects to the management server to which you want the client computer to connect. The communications file is the Sylink.xml file.

[Exporting the client-server communications file \(Sylink.xml\) manually](#)

2. Copy the communication file to the client computer.

You can either save the file to a network location, email it to the user on the client computer, or copy it to removable media.

3. Do one of the following tasks:

- In the full product installation file from the [Broadcom Download Center](#), locate Tools\SylinkDrop\SylinkDrop.exe.
- On the computer that runs the management server, locate C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\Version.Number\Bin\SylinkDrop.exe

You can run the tool remotely or save it and then run it on the client computer. For information on the command-line options, in the \Tools\SylinkDrop folder, click the readme file.

4. In the **Sylink Drop** dialog box, click **Browse**, and locate the .xml file you deployed in step 2 to the client computer.
5. Click **Update Sylink**.
6. When you see a confirmation dialog box, click **OK**.
7. In the **Sylink Drop** dialog box, click **Exit**.

## Troubleshooting the Symantec Linux Agent

In the table below you find the resources for troubleshooting the Symantec Agent for Linux (as of 14.3 RU1).

Action	Description
Checking the status of the agent.	To check the version and connection status of the agent and to confirm that the modules are loaded and daemons are running, navigate to <code>/usr/lib/symantec</code> and run the following command: <code>./status.sh</code>
Checking the versions of the agent packages.	Navigate to <code>/usr/lib/symantec</code> and run the following command: <code>./version.sh</code>
Viewing the logs.	You find the Symantec Linux Agent logs at the following locations: <ul style="list-style-type: none"> <li>• <b>AMD log</b> - provides information related to scanning. <code>/var/log/sdcsslog/amdlog</code></li> <li>• <b>CAF log</b> - provides information related to agent activities such as communication with the server, enrollment, commands, events, etc. <code>/var/log/sdcss-caflog/</code></li> <li>• <b>Agent log</b> - provides information related to agent activities. <code>/var/log/sdcsslog/SISIDSEvents*.csv</code></li> <li>• <b>CVE log</b> - provides information related to communication between Symantec Endpoint Protection Manager and the agent. <code>/var/log/sdcss-caflog/cve.log</code></li> </ul>
Collecting the logs into a zip file.	You can use <code>GetAgentInfo</code> script to collect all log files into a ZIP file that you can send to customer support. <ol style="list-style-type: none"> <li>1. Login to Symantec Linux Agent system.</li> <li>2. Navigate to <code>/opt/Symantec/sdcssagent/IPS/tools/</code>.</li> <li>3. Run <code>./getagentinfo.sh</code> as root.</li> <li>4. A ZIP file will be created in <code>/tmp/</code> directory. The name of the file will look similar to <code>20201208_184935_0001_CU_mihsan-rhel8.zip</code> <code>-out &lt;directory&gt;</code> lets you change the location and the name of the generated ZIP file.</li> </ol>
Changing the CVE logging level.	By default, the CVE logging level is <code>info</code> . You can change the logging level to <code>ebug</code> in the <code>/opt/Symantec/cafagent/bin/log4j.properties</code> file. After changing the file, you must restart the <code>cafagent</code> service.
Changing the AMD logging level.	By default, the AMD logging level is <code>info</code> . You can change the logging level to <code>trace</code> , to <code>warning</code> , or to <code>error</code> in the <code>/opt/Symantec/sdcssagent/AMD/system/AntiMalware.ini</code> file. <b>Note:</b> Before you modify the <code>AntiMalware.ini</code> file, stop the <code>sisamdagent</code> : <b>Note:</b> <code>service sisamdagent stop</code> <b>Note:</b> After you modify the file, restart the service: <b>Note:</b> <code>service sisamdagent start</code>

---

## Troubleshooting communication problems between Symantec Endpoint Protection Manager and the console or the default database

If you have a connection problem with the Symantec Endpoint Protection Manager console or the default database, you may see one of the following symptoms:

- The management server service (semsrv) stops.
- The management server service does not stay in a started state.
- The Home, Monitors, and Reports pages display an HTTP error.
- The Home, Monitors, and Reports pages are blank.
- The Home, Monitors, and Reports pages display a continuously loading progress bar, without displaying any content.

All of these issues display a Java -1 error in the Windows Event log. To find the specific cause for the Java -1 error, look in the scm-server log. The scm-server log is located by default in the following location:

```
SEPM_Install\tomcat\logs\scm-server-0.log
```

The default for SEPM\_Install is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager.

**Table 192: Checking the communication with the console or database**

What to check	Description
Test the connectivity between the database and the management server.	You can verify that the management server and the database communicate properly. <a href="#">Verifying the connection with the database</a>
Check that the management server heap size is correct.	If you cannot log on to the management server's remote console, you may need to increase the Java heap size. You may also see an out-of-memory message in the scm-server log. For more information on the default heap sizes, see: <a href="#">Determining the default settings for the network sizes that you select during installation of the Symantec Endpoint Protection Manager</a>
Check that the management server is not running multiple versions of PHP.	You can check whether the management server runs multiple software packages that use different versions of PHP. PHP checks for a global configuration file (php.ini). If there are multiple configuration files, you must force each product to use its own interpreter. When each product uses the correct version of PHP associated with it, the management server operates properly.
Check the system requirements.	You can check whether both the client and the management server run the minimum or the recommended system requirements. For the most current system requirements, see: <a href="#">Release notes, new fixes, and system requirements for all versions of Endpoint Protection</a>

### Verifying the management server connection with the database

The management server and the database may not communicate properly. You should verify that the database runs and then test the connection between the server and the database.

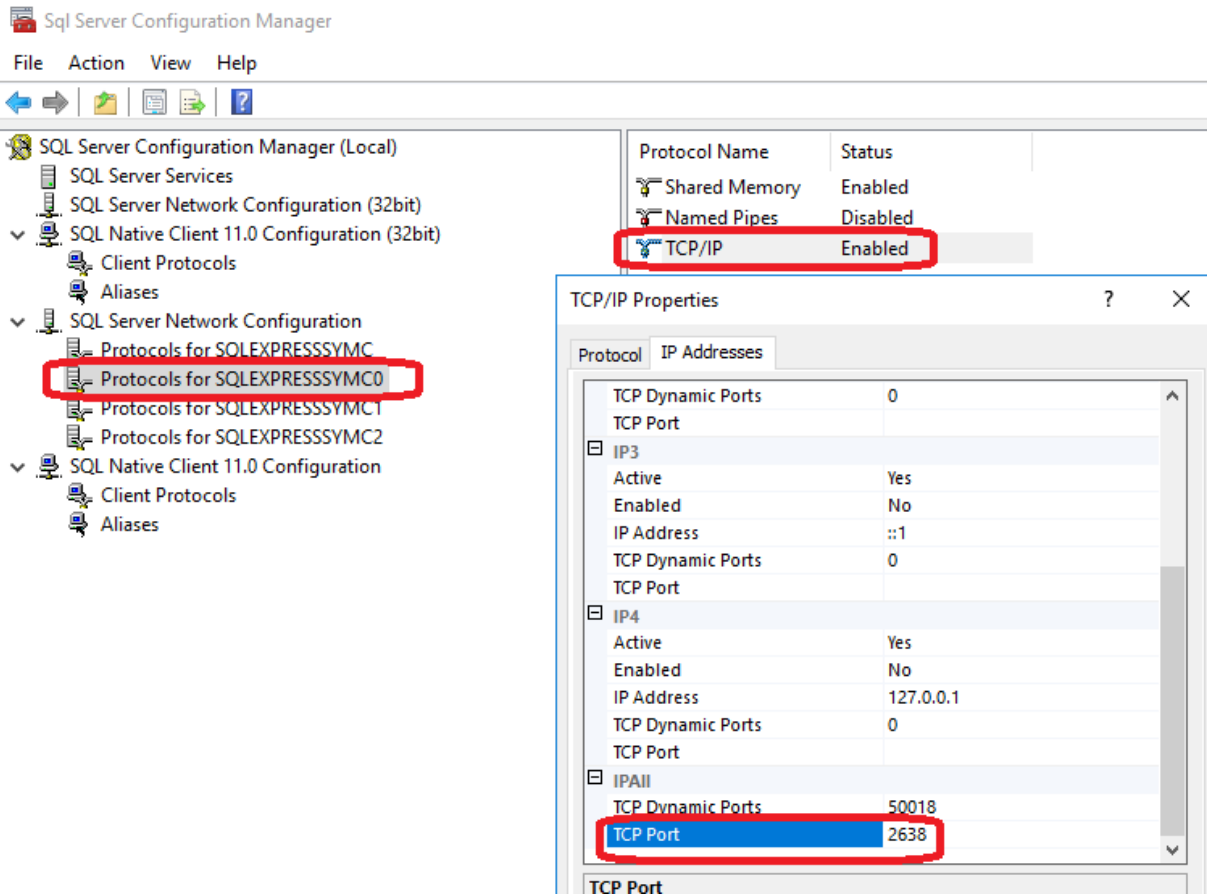
**Table 193: Verifying the database connection**

Database type	Perform these steps
Microsoft SQL Server Express database (as of 14.3 RU1)	<ul style="list-style-type: none"><li>• Verify that the SQL Server Express service runs and that the sqlserver.exe process listens to TCP port 2638.</li><li>• Test the ODBC connection.</li></ul>
Embedded Sybase database (14.3 MP1 and earlier)	<ul style="list-style-type: none"><li>• Verify that the Symantec Embedded Database service runs and that the dbsrv9.exe process listens to TCP port 2638.</li><li>• Test the ODBC connection.</li></ul>
Remote Microsoft SQL Server database	<ul style="list-style-type: none"><li>• Verify that you have specified a named instance when you installed and configured Symantec Endpoint Protection Manager.</li><li>• Verify that SQL Server runs and is properly configured.</li><li>• Verify that the network connection between management server and the SQL database is correct.</li><li>• Test the ODBC connection.</li></ul>

**To verify communication with the Microsoft SQL Server Express database:**

1. On the **Start** menu, expand **Microsoft SQL Server 2017** and click **SQL Server 2017 Configuration Manager**.
2. In the **SQL Server Configuration Manager** dialog box, expand **SQL Server Network Configuration**, and select the **Protocols for SQLEXPRESS** instance.  
The **TCP/IP** field should be set to **Enabled**.
3. Right-click **TCP/IP**, and then click **Properties**.
4. On the IP Addresses tab, scroll down to the **IPAll** category; the **TCP Port** field displays the port number, 2638 by default.





#### To verify communication with the embedded database:

1. On the management server computer, click **Start > Control Panel > Administrative Tools**.
2. In the **Administrative Tools** dialog box, double-click **Data Sources (ODBC)**.
3. In the **ODBC Data Source Administrator** dialog box, click **System DSN**.
4. On the **System DSN** tab, double-click **SymantecEndpointSecurityDSN**.
5. On the **ODBC** tab, verify that the Data source name drop-down list is `SymantecEndpointSecurityDSN` and type an optional description.
6. Click **Login**.
7. On the **Login** tab, in the **User ID** text box, type `dba`.
8. In the **Password** text box, type the password for the database.  
This password is the one that you entered for the database when you installed the management server.
9. Click **Database**.
10. On the **Database** tab, in the **Server name** text box, type:  
`\\servername\instancename`  
If you use the English version of Symantec Endpoint Protection Manager, type the default, `sem5`. Otherwise, leave the Server name text box blank.
11. On the **ODBC** tab, click **Test Connection** and verify that it succeeds.
12. Click **OK**.
13. Click **OK**.

---

### To verify communication to the Microsoft SQL Server database:

1. On the management server computer, click **Start > Control Panel > Administrative Tools**.
2. In the **Administrative Tools** dialog box, double-click **Data Sources (ODBC)**.
3. In the **ODBC Data Source Administrator** dialog box, click **System DSN**.
4. On the **System DSN** tab, double-click **SymantecEndpointSecurityDSN**.
5. In the **Server** drop-down list, verify that the correct server and instance is selected.
6. Click **Next**.
7. For Login ID, type `sa`.
8. In the **Password** text box, type the password for the database.  
This password is the one that you entered for the database when you installed the management server.
9. Click **Next** and make sure that `sem5` is selected for the default database.
10. Click **Next**.
11. Click **Finish**.
12. Click **Test Data Source** and look for the result that states:  
`TESTS COMPLETED SUCCESSFULLY!`

## Client and server communication files

The communication settings between the client and server and other client settings are stored in files on the client computer.

**Table 194: Client files**

File name	Description
SerDef.dat	An encrypted file that stores communication settings by location. Each time the user changes locations, the SerDef.dat file is read and the appropriate communication settings for the new location are applied to the client.
sylink.xml	Stores the global communication settings. This file is for internal use only and should not be edited. It contains settings from the Symantec Endpoint Protection Manager. If you edit this file, most settings will be overwritten by the settings from the management server the next time the client connects to the management server.
SerState.dat	An encrypted file that stores information about the user interface, such as the client's screen size, whether the client's console for Network and Host Exploit Mitigation appears, and whether Windows services appear. When the client starts, it reads this file and returns to the same user interface state as before it was stopped.

## Troubleshooting reporting issues

### You should be aware of the following information when you use reports:

- Timestamps, including client scan times, in reports and logs are given in the user's local time. The reporting database contains events in Greenwich Mean Time (GMT). When you create a report, the GMT values are converted to the local time of the computer on which you view the reports.
- If managed clients are in a different time zone from the management server, and you use the **Set specific dates** filter option, you may see unexpected results. The accuracy of the data and the time on both the client and the management server may be affected.
- If you change the time zone on the server, log off of the console and log on again to see accurate times in logs and reports.
- In some cases, the report data does not have a one-to-one correspondence with what appears in your security products. This lack of correspondence occurs because the reporting software aggregates security events.
- You can use SSL with the reporting functions for increased security. SSL provides confidentiality, the integrity of your data, and authentication between the client and the server.

---

See the article: [Enabling SSL communications between a Symantec Endpoint Protection Manager and its clients](#)

- Risk category information in the reports is obtained from the Symantec Security Response Web site. Until the Symantec Endpoint Protection Manager console is able to retrieve this information, any reports that you generate show Unknown in the risk category fields.
- The reports that you generate give an accurate picture of compromised computers in your network. Reports are based on log data, not the Windows registry data.
- If you get database errors when you run a report that includes a large amount of data, you might want to change database timeout parameters.

[Changing timeout parameters for reviewing reports and logs](#)

- If you get CGI or terminated process errors, you might want to change other timeout parameters. For more information, see the following document in the following article: [SEPM Reporting does not respond or shows a timeout error message when querying large amounts of data](#).
- If you have disabled the use of loopback addresses on the computer, the reporting pages do not display. [Accessing reporting pages when the use of loopback addresses is disabled](#)

## Changing timeout parameters for reviewing reports and logs

If database errors occur when you view either reports or logs that contain a lot of data, you can make the following changes:

- Change the database connection timeout
- Change the database command timeout

The reporting defaults for these values are as follows:

- Connection timeout is 300 seconds (5 minutes)
- Command timeout is 300 seconds (5 minutes)

1. To change database timeout values in Reporter.php, browse to the following default folder on the Symantec Endpoint Protection Manager server:

C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Php\Include\Resources

2. Open the Reporter.php file with a plain-text editor, such as Notepad.

3. Find the **\$CommandTimeout** and **\$ConnectionTimeout** lines and increase the value (in seconds). If either line does not exist, create it. For example, to increase the timeout period to 10 minutes, change the line to the following value:

```
$CommandTimeout = 600;
```

```
$ConnectionTimeout = 600;
```

Add these new lines before the following characters: ?>

4. Save and close the Reporter.php file.

### NOTE

If you specify zero, or leave the fields blank, the default setting is used.

If you get CGI or terminated process errors, you might want to change the following parameters:

- max\_execution\_time parameter in the Php.ini file
  - The Apache timeout parameters, FcgidIOTimeout, FcgidBusyTimeout, and FcgidIdleTimeout, in the httpd.conf file
5. To change the max\_execution\_time parameter in Php.ini, browse to following default folder on the Symantec Endpoint Protection Manager server:

C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Php

- 
6. Right-click the Php.ini file, and then click **Properties**.
  7. On the **General** tab, uncheck **Read-only**.
  8. Click **OK**.
  9. Open the Php.ini file with a plain-text editor, such as Notepad.
  10. Locate the **max\_execution\_time** entry and increase the value (in seconds). For example, to increase the timeout to 10 minutes, change the line to the following value:  
`max_execution_time=600`
  11. Save and close the Php.ini file.
  12. Right-click the Php.ini file, and then click **Properties**.
  13. On the **General** tab, check **Read-only**.
  14. Click **OK**.
  15. To change Apache timeout parameters in httpd.conf, browse to the following default folder on the Symantec Endpoint Protection Manager server:  
`C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\apache\conf`
  16. Open the httpd.conf file with a plain-text editor, such as Notepad.
  17. Locate the following lines and increase the values (in seconds):
    - `FcgidIOTimeout 1800`
    - `FcgidBusyTimeout 1800`
    - `FcgidIdleTimeout 1800`
  18. Save and close the httpd.conf file.

## Accessing reporting pages when the use of loopback addresses is disabled

If you have disabled the use of loopback addresses on the computer, the reporting pages do not display. If you try to log on to the Symantec Endpoint Protection Manager console or to access the reporting functions, you see the following error message:

### Unable to communicate with Reporting component

The **Home**, **Monitors**, and **Reports** pages are blank; the **Policies**, **Clients**, and **Admin** pages look and function normally.

To get the **Reports** components to display when you have disabled loopback addresses, you must associate the word **localhost** with your computer's IP address. You can edit the Windows hosts file to associate localhost with an IP address.

### [Logging on to reporting from a standalone web browser](#)

To associate localhost with the IP address on computers running Windows

1. Change directory to the location of your hosts file.  
By default, the hosts file is located in `%SystemRoot%\system32\drivers\etc`
2. Open the hosts file with an editor.
3. Add the following line to the hosts file:  
`IPAddress localhost #to log on to reporting functions`

---

where you replace IPAddress with your computer's IP address. You can add any comment you want after the pound sign (#). For example, you can type the following line:

192.168.1.100 localhost # This entry is the IPv4 for my console computer

2001:db8:85a3::8a2e:370:7334 localhost # This entry is the IPv6 address for my console computer

IPv6 is supported as of version 14.2.

4. Save and close the file.

## What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console

Power Eraser provides aggressive scanning and analysis to help resolve issues with heavily infected Windows computers. Because Power Eraser analysis is aggressive, it sometimes flags the critical files that you might need. Power Eraser can produce more false positives than virus and spyware scans.

### WARNING

You should run Power Eraser only in emergency situations, such as when computers exhibit instability or have a persistent problem. Typically, you run Power Eraser on a single computer or small group of computers. You should not run other applications at the same time. In some cases, a regular scan event alerts you to run a Power Eraser analysis.

### Differences between using Power Eraser from Symantec Endpoint Protection Manager or locally with the SymDiag tool

**You can run Power Eraser remotely from the management console on your Windows clients. Symantec Endpoint Protection does not include an option to launch Power Eraser directly from the client. However, a user on the client computer can download the SymDiag tool and run Power Eraser from the tool.**

- If you use the SymDiag tool, Power Eraser detections do not appear in the Symantec Endpoint Protection Manager logs.
- When you run Power Eraser from the console, Power Eraser does not examine the user-specific load points, registrations, and folders that the SymDiag tool examines.

### NOTE

Make sure that you do not run Power Eraser from the console and locally with the SymDiag tool at the same time. Otherwise, you might negatively affect the computer performance.

Power Eraser consumes a large amount of computer resources. Power Eraser files can also consume a large amount of space on the computer if you run Power Eraser on a computer multiple times. During each analysis, Power Eraser saves detection information in the files that it stores in the Symantec Endpoint Protection application folder. The files are purged when the client purges the logs.

### How Power Eraser is different from virus and spyware scans

**Power Eraser is different from regular scans in the following ways:**

- Unlike a full scan, Power Eraser does not scan every file on the computer. Power Eraser examines load points and load point disk locations as well as running processes and installed services.
- Power Eraser detections do not appear in the Quarantine.
- Power Eraser takes precedence over virus and spyware scans. When you run Power Eraser, Symantec Endpoint Protection cancels any virus and spyware scan in progress.
- Power Eraser does not automatically remediate detections. You must review the detection list in the Scan log or Risk log and select an action from the log. You can choose to remove the detection or mark the detection as safe (leave alone). You can also restore (undo) a removed detection.

---

Power Eraser can run in regular mode or in rootkit mode. The rootkit mode requires a restart before the scan launches. Also, if you choose to remove any Power Eraser detection, the computer must be restarted for the remediation to complete.

## Overview of the high-level steps that you perform when you need to run Power Eraser

### You perform two high-level steps when you run Power Eraser from the console:

- Start a Power Eraser analysis on one computer or a small group of computers. Power Eraser does not automatically remediate any detections because of the potential for false positives.
- Use the Risk log or Scan log to review Power Eraser detections and manually request that Power Eraser remove any detections that you determine are threats. You can also acknowledge the detections that you want to ignore and leave alone.

Review the workflow for details about how to run Power Eraser from the console and how to make sure that you configure the console settings correctly.

### [Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console](#)

## Overview of the Symantec Endpoint Protection Manager policy settings that affect Power Eraser

### The following are the policy settings that affect Power Eraser:

- Scan settings for user interaction  
When you let users cancel any virus and spyware scan, you also let them cancel any Power Eraser analysis. However, users cannot pause or snooze Power Eraser.  
[Allowing users to view scan progress and interact with scans on Windows computers](#)
- Exceptions policy  
Power Eraser honors the following virus and spyware exceptions: file, folder, known risk, application, and trusted web domain. Power Eraser does not honor extension exceptions.  
[Creating exceptions for Virus and Spyware scans](#)
- Log retention settings  
You can take action on Power Eraser detections as long as the detections appear in the logs. The logs are purged after the period of time that is specified in the Virus and Spyware Protection policy. By default, log events are available for 14 days. You can modify the log retention setting, or after the events expire, you can run another scan and re-populate the logs.  
[Modifying log handling and notification settings on Windows computers](#)
- Restart options  
You can configure the restart settings specifically for rootkit analysis when you choose to run Power Eraser in rootkit detection mode. The administrator must have restart privileges. After you choose to remove a Power Eraser detection, the computer uses the group restart settings. Power Eraser does not use the rootkit restart settings to restart and complete a remediation.  
[Restarting the client computers from Symantec Endpoint Protection Manager](#)
- Reputation queries  
Power Eraser uses the Symantec Insight server in the cloud when it scans and makes decisions about files. If you disable reputation queries, or if the client computer cannot connect to the Insight server, Power Eraser cannot use Symantec Insight. Without Symantec Insight, Power Eraser makes fewer detections, and the detections it makes are more likely to be false positives. Reputation queries are enabled when the **Allow Insight lookups for threat detection** option is enabled. The option is enabled by default.  
[How Symantec Endpoint Protection uses Symantec Insight to make decisions about files](#)
- Submissions  
Symantec Endpoint Protection sends the information about Power Eraser detections to Symantec when the **Antivirus detections** option is enabled. The option is enabled by default.  
[Understanding server data collection and client submissions and their importance to the security of your network](#)

## Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console

Typically you need to run a Power Eraser analysis when the Risk log shows a failed repair and recommends that you run Power Eraser. You also might run Power Eraser when a computer becomes unstable and appears to have malware or a virus that cannot be removed.

### WARNING

Use Power Eraser carefully. The analysis is aggressive and prone to false positives.

### What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console

You can run Power Eraser from Symantec Endpoint Protection Manager on Windows client computers only.

### NOTE

Power Eraser runs in one of two modes: without rootkit detection or with rootkit detection. The rootkit detection analysis requires a restart. The administrator must have restart privileges to run Power Eraser with rootkit detection.

**Table 195: Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console**

Task	Description
Set administrator privileges to run Power Eraser	<b>To run Power Eraser on client computers, administrators must have the following command access rights:</b> <ul style="list-style-type: none"><li>• <b>Start Power Eraser Analysis</b></li><li>• <b>Restart Client Computers</b> (required to run Power Eraser with rootkit detection)</li></ul> <a href="#">Adding an administrator account and setting access rights</a>
Set the log retention policy	The log retention setting affects how long the events are available for you to perform the Power Eraser remediate and restore actions. You can modify the log retention setting if you want more time to consider these actions. Alternately, you can run Power Eraser again to re-populate the logs. The log retention setting is part of the miscellaneous options in the Virus and Spyware Protection policy. <a href="#">Modifying log handling and notification settings on Windows computers</a>
Make sure that your clients have Internet connectivity	Your client computers require Internet access so that Power Eraser can use Symantec Insight reputation data to make decisions about potential threats. Intermittent or non-existent Internet access means that Power Eraser cannot use Symantec Insight. Without Symantec Insight, Power Eraser makes fewer detections, and the detections it produces are more likely to be false positives.

Task	Description
Start a Power Eraser analysis on a client computer from Symantec Endpoint Protection Manager	<p>Choose whether to run Power Eraser in regular mode or rootkit mode.</p> <p><b>You can issue the Power Eraser command from several places in Symantec Endpoint Protection Manager:</b></p> <ul style="list-style-type: none"> <li>• <b>Clients</b> page</li> <li>• Computer Status log</li> <li>• Risk log</li> </ul> <p><b>Note:</b> A user on the client computer cannot run Power Eraser directly from the client user interface. Power Eraser is available as part of the SymDiag tool. However, if a client user runs the tool, the resulting logs that include Power Eraser detections are not sent to Symantec Endpoint Protection Manager.</p> <p><a href="#">Starting Power Eraser analysis from Symantec Endpoint Protection Manager</a></p> <p>You can view the status of the command in the Computer Status log. You can filter the log so that only Power Eraser commands appear for ease of viewing.</p> <p>After you run Power Eraser, you view the results in the Scan log or the Risk log. The Scan log shows whether or not scan results are pending.</p>
Cancel a Power Eraser command or action on a client computer	<p>To cancel the Power Eraser command, use the Command Status log.</p> <p><b>Note:</b> You cannot cancel Power Eraser running in rootkit mode after the restart prompt appears on the client computer. After the restart, only the computer user can cancel Power Eraser if the Virus and Spyware Protection policy lets users cancel scans.</p> <p>If you cancel the Power Eraser command, you also cancel any pending actions that are associated with any Power Eraser analysis, including any remediation or undo actions.</p> <p><a href="#">Running commands on client computers from the console</a></p>
View Power Eraser detections from the logs	<p><b>You can view Power Eraser detections from the following logs in Symantec Endpoint Protection Manager:</b></p> <ul style="list-style-type: none"> <li>• Scan log <p>The Scan log has a <b>Scan type</b> filter to display only Power Eraser results. The view also indicates whether or not scan results are pending. You can select <b>Detections</b> in the filtered view to display the <b>Power Eraser Detections</b> view.</p> </li> <li>• Risk log <p>The Risk log provides a similar filter for Power Eraser detections. However, the Risk log does not show whether or not scan results are pending.</p> </li> <li>• Computer Status log <p>The Computer Status log might include report icons in the <b>Infected</b> column. The event details icon links to a report that shows all current threats that cannot be remediated. The report includes log-only detections and unresolved detections. The report might recommend that you run Power Eraser on some computers.</p> <p>A Power Eraser icon links to a report that shows any Power Eraser detections on the computer that require administrator action.</p> <p>These icons also appear in the <b>Health State</b> column on the <b>Clients</b> page.</p> <p><a href="#">Viewing logs</a></p> </li> </ul>
Check for the notifications that recommend that you run Power Eraser on client computers	<p>By default, the administrator receives a notification when a regular scan cannot repair an infection and Power Eraser is recommended. You can check for the <b>Power Eraser recommended</b> notification on the <b>Monitors &gt; Notifications</b> page.</p> <p><a href="#">Viewing and acknowledging notifications</a></p>



Task	Description
View Power Eraser detections on the <b>Command Status</b> page	<p>You can access reports about Power Eraser detections on the <b>Command Status</b> page. An event details icon appears in the <b>Completion Status</b> column. The icon links to a report that shows information about detections that were made by the <b>Start Power Eraser Analysis</b> command and any other scan command.</p> <p>The command status details option gives you information about a particular scan. You can click on the event details icon to get information about a particular client computer.</p> <p><a href="#">Running commands on client computers from the console</a></p>
View Power Eraser detections from the <b>Clients</b> tab	<p>You can access reports about Power Eraser detections from the <b>Clients</b> tab on the <b>Clients</b> page. Report icons appear in the <b>Health State</b> column if information is available. The event details icon links to a report that shows all current threats that cannot be remediated. The report includes any Power Eraser detections.</p> <p>A Power Eraser icon links to a report that shows any Power Eraser detections on the computer that require administrator action.</p> <p>The icons also appear in the Computer Status log.</p> <p><a href="#">Viewing the protection status of client computers</a></p>
Remediate or restore Power Eraser detections from the Scan log or Risk log in Symantec Endpoint Protection Manager	<p>Unlike other Symantec Endpoint Protection scans, Power Eraser does not automatically remediate detected threats. Power Eraser analysis is aggressive and might detect many false positives. After you determine that the detection requires remediation, you must initiate a remediation manually.</p> <p>You can also undo (restore) a Power Eraser detection that you remediated.</p> <p><a href="#">Responding to Power Eraser detections</a></p>

## Starting Power Eraser analysis from Symantec Endpoint Protection Manager

You can run Power Eraser to analyze and detect persistent threats on a single computer or a small group of computers.

[What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console](#)

After Power Eraser detects potential risks, you view the risks and determine which risks are threats. Power Eraser does not automatically remediate risks. You must manually run Power Eraser to remediate the risks that you determine are threats. You can also run Power Eraser on a particular threat or threats that other protection features detect. Power Eraser runs on the computers that are associated with the detection.

[Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console](#)

[Responding to Power Eraser detections](#)

### NOTE

When you run Power Eraser in rootkit mode, and the restart option message appears on the client computer, the administrator or the user cannot cancel Power Eraser. After the restart, the user can cancel Power Eraser if the Virus and Spyware Protection policy lets users cancel scans.

1. To start Power Eraser analysis from the **Clients** page in Symantec Endpoint Protection Manager, on the **Clients** page, on the **Clients** tab, select the computers that you want to analyze.

If you select many computers, you might adversely affect the performance of your network.

- 
2. Under **Tasks**, click **Run command on computers**, and then click **Start Power Eraser Analysis**.
  3. In the **Choose Power Eraser** dialog, select whether or not you want Power Eraser to run in rootkit mode. For rootkit mode, you can set the restart options. You must have administrator privileges to set restart options and run a rootkit scan.
  4. Click **OK**.

Power Eraser runs on the select computers. You can cancel the command on the **Command Status** tab on the **Monitors** page.
  5. To start Power Eraser analysis from the Computer Status log in Symantec Endpoint Protection Manager, in the console, in the sidebar, click **Monitors** and select the **Logs** tab.
  6. In the **Log type** list box, select the **Computer Status** log, and then click **View Log**.
  7. Select the computers on which you want to run Power Eraser and select **Start Power Eraser Analysis** from the **Commands** drop-down box.

If you select many computers, you might adversely affect the performance of your network.
  8. Click **Start**.
  9. In the **Choose Power Eraser** dialog, select whether or not you want Power Eraser to run in rootkit mode. For rootkit mode, you can set the restart options. You must have administrator privileges to set restart options and run a rootkit scan.
  10. Click **OK**.

Power Eraser runs on the selected computers. You can cancel the command on the **Command Status** tab.
  11. To start Power Eraser analysis from the Risk log in Symantec Endpoint Protection Manager, in the console, in the sidebar, click **Monitors** and select the **Logs** tab.
  12. In the **Log type** list box, select the **Risk** log, and then click **View Log**.
  13. Select the risks on which you want to run Power Eraser. In the **Event Action** column, you might see an alert to run Power Eraser.

You can run Power Eraser on any risk in the log.
  14. Select **Start Power Eraser Analysis** from the **Action** drop-down or the **Action** column.
  15. Click **Start**.
  16. In the **Choose Power Eraser** dialog, select whether or not you want Power Eraser to run in rootkit mode. For rootkit mode, you can set the restart options. You must have administrator privileges to set restart options and run a rootkit scan.
  17. Click **OK**.

Power Eraser runs on the computers that are infected with the selected risks. You can cancel the command on the **Command Status** tab.

## Responding to Power Eraser detections

Power Eraser does not remediate any detections during a scan because its aggressive detection capability is prone to false positives. You must request remediation for detected events from the logs after you review the detections and decide whether to remediate them or leave them alone. If you choose remediation, Power Eraser removes the files that are associated with the detection. However, you can restore the removed files until the logs are purged.

The log retention policy determines how long Power Eraser events are available. By default, the events are available for 14 days.

---

## Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console

### What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console

To respond to Power Eraser detections

1. Make sure that the Power Eraser analysis completed.
  - The Computer Status log includes an icon that indicates the scan is complete.
  - The Scan log shows whether or not Power Eraser finished the analysis.
2. In the Risk log or on the **Scan log > View detections** page, select a single detection or multiple detections to which to apply an action.
  - Next to a particular risk that is labeled **Potential risk found (Pending admin action)**, click the plus icon in the **Action** column.
  - Select multiple risks that are labeled **Potential risk found (Pending admin action)**, and then select the action from the **Action** drop-down menu.
3. Choose one of the following actions:
  - **Delete risk that Power Eraser detected**  
Remediates the risk by removing it from the computer. Power Eraser saves a safe backup file that can be restored.
  - **Ignore risk that Power Eraser detected**  
Acknowledges that you reviewed the detection and do not want to remediate the risk.

#### NOTE

This action changes the event action to “Left alone by Admin” in the management console logs only.  
The acknowledgement does not update the corresponding event action on the client. The client log view continues to show the event action as “Pending analysis.”

4. If you selected an action from the **Action** drop-down menu, click **Apply**.

If you selected **Ignore risk that Power Eraser detected**, the detection now appears as **Potential risk found (left alone)**.

You can restore a removed detection that is labeled **Potential risk found (Removed)** by selecting the **Restore risk that Power Eraser deleted** action.

**Table 196: Summary of Power Eraser detection states**

Detection state	Description
<b>Pending admin action</b>	Power Eraser detected the risk as a potential threat. You should review the risk and decide if Power Eraser should remediate the risk or acknowledge the risk and leave it alone.
<b>Restored</b>	An administrator restored any files that were moved when an administrator requested that Power Eraser remediate the risk.
<b>Deleted</b>	An administrator requested that Power Eraser remediate and delete the risk. When Power Eraser deletes a risk, it deletes the files that are associated with the risk but makes safe backup copies that can be restored. You might want to restore a deleted risk that you later determine is not a risk. You can restore the files until the log events are purged.
<b>Left alone by admin</b>	An administrator requested that Power Eraser leave the risk alone.

---

## Appendices

---

Get reference information about client feature comparison, tools, command-line options, third-party installation tools

This section includes a comparison of client features, tools included with Symantec Endpoint Protection, client command-line options, Windows installation with third-party tools, and more.

### Symantec Endpoint Protection features based on platform

- [Client protection features based on platform](#)
- [Management server features based on platform](#)
- [AutoUpgrade features based on platform](#)
- [Virus and Spyware Protection policy settings based on platform](#)
- [Intrusion Prevention policy and Memory Exploit Mitigation policy settings based on platform](#)
- [LiveUpdate policy settings based on platform](#)
- [Web and Cloud Access Protection policy settings based on platform \(was Integrations and then Network Traffic Redirection\)](#)
- [Exceptions policy settings based on platform](#)
- [Device Control differences based on platform](#)

[How to choose a client installation type](#)

[Symantec Endpoint Protection feature dependencies for Windows clients \(12.1.x through 14.x\)](#)

#### Client protection features based on platform

**Table 197: Client protection features based on platform**

Client feature	Windows	Mac	Linux
Virus and Spyware Protection	Yes	Yes	Yes
Network and Host Exploit Mitigation <ul style="list-style-type: none"><li>• Network Threat Protection (intrusion prevention and firewall)</li><li>• Memory Exploit Mitigation (introduced as Generic Exploit Mitigation in 14)</li></ul>	Yes	<ul style="list-style-type: none"><li>• Firewall (as of 14.2)</li><li>• Intrusion prevention (as of 12.1.4)</li></ul> Intrusion prevention for the Mac does not support custom signatures.	No
Proactive Threat Protection <ul style="list-style-type: none"><li>• Application and Device Control</li><li>• SONAR</li></ul>	Yes	Device Control only (as of 14)	No
Host Integrity	Yes	No	No
Other protections <ul style="list-style-type: none"><li>• System lockdown</li><li>• Tamper Protection</li></ul>	Yes	No	No

[About application control, system lockdown, and device control](#)

[How Host Integrity works](#)

## Management features based on platform

**Table 198: Management features based on platform**

Management feature	Windows	Mac	Linux
Deploy clients remotely from Symantec Endpoint Protection Manager <ul style="list-style-type: none"> <li>• Web link and email</li> <li>• Remote push</li> <li>• Save package</li> </ul>	Yes	Yes	Yes ( <b>Web link and email, Save package</b> only)
Run commands on clients from the management server	<ul style="list-style-type: none"> <li>• Scan</li> <li>• Update content</li> <li>• Update content and scan</li> <li>• Start Power Eraser analysis (as of 12.1.5)</li> <li>• Restart client computers</li> <li>• Enable Auto-Protect</li> <li>• Enable Network Threat Protection</li> <li>• Disable Network Threat Protection</li> <li>• Enable Download Insight</li> <li>• Disable Download Insight</li> <li>• Collect File Fingerprint List (as of 12.1.6)</li> <li>• Delete from Quarantine**</li> <li>• Cancel all scans**</li> </ul>	<ul style="list-style-type: none"> <li>• Scan</li> <li>• Update content</li> <li>• Update content and scan</li> <li>• Restart client computers (hard restart only)</li> <li>• Enable Auto-Protect</li> <li>• Enable Network Threat Protection (as of 12.1.4)</li> <li>• Disable Network Threat Protection (as of 12.1.4)</li> </ul>	<ul style="list-style-type: none"> <li>• Scan</li> <li>• Update content</li> <li>• Update content and scan</li> <li>• Enable Auto-Protect</li> </ul>
Enable learned applications and Network Application Monitoring	Yes	No	No
Create locations and set security policies that apply by location	Yes	Yes	No You can view the client's location by the command line, but the client does not automatically switch locations based on specific criteria.
Set restart options for clients	Yes	No	No
Quick reports and Scheduled reports	<ul style="list-style-type: none"> <li>• Audit</li> <li>• Application and Device Control</li> <li>• Compliance</li> <li>• Computer status</li> <li>• Deception (14.0.1)</li> <li>• Network and Host Exploit Mitigation</li> <li>• Risk</li> <li>• Scan</li> <li>• System</li> </ul>	<ul style="list-style-type: none"> <li>• Computer status</li> <li>• Network and Host Exploit Mitigation</li> <li>• Risk</li> <li>• Scan</li> </ul>	<ul style="list-style-type: none"> <li>• Audit</li> <li>• Computer status</li> <li>• Risk</li> <li>• Scan</li> <li>• System</li> </ul>

Management feature	Windows	Mac	Linux
Set size and retention options for logs that are maintained on the client computers	<ul style="list-style-type: none"> <li>• System</li> <li>• Security and risk</li> <li>• Security</li> <li>• Traffic</li> <li>• Packet</li> <li>• Control</li> </ul>	<ul style="list-style-type: none"> <li>• System</li> <li>• Security and risk</li> <li>• Security</li> </ul>	<ul style="list-style-type: none"> <li>• System</li> <li>• Security and risk</li> </ul>
Password protecting the client	Yes	Uninstall the client (14.0.1)	No
Move clients to a different management server by running the SylinkDrop tool	Yes	Yes	No
Move clients to a different management server by redeploying a client package with the <b>Communication update package deployment</b> option	Yes	Yes	No
Configure client submissions of pseudonymous security information to Symantec	Yes	(12.1.4 and later) The Submissions setting only controls antivirus detection information. You can manually disable or enable intrusion prevention submissions on the clients. <a href="#">How to disable IPS data submission on Symantec Endpoint Protection for Mac clients</a>	No
Configure clients to securely submit pseudonymous system and usage information	Yes	No	No
Manage the external communication between the management server and the clients	Yes	For LiveUpdate only	No
Manage client communication settings	<ul style="list-style-type: none"> <li>• Management server lists</li> <li>• Communication mode (push or pull)</li> <li>• Set heartbeat interval</li> <li>• Upload learned applications</li> <li>• Upload critical events immediately</li> <li>• Set download randomization</li> <li>• Set reconnection preferences</li> </ul>	<ul style="list-style-type: none"> <li>• Management server lists</li> <li>• Communication mode (push or pull)</li> <li>• Set heartbeat interval</li> <li>• Set download randomization</li> <li>• Set reconnection preferences</li> </ul>	<ul style="list-style-type: none"> <li>• Management server lists</li> <li>• Communication mode (push or pull)</li> <li>• Set heartbeat interval</li> </ul>

Management feature	Windows	Mac	Linux
Configure clients to use private servers (12.1.6) <ul style="list-style-type: none"> <li>Endpoint Detection and Response server for Insight lookups and submissions</li> <li>Private Insight server for Insight lookups</li> </ul>	Yes	No	No
Automatically upgrade the Symantec Endpoint Protection client with AutoUpgrade	Yes	Yes (14)	No
Automatically uninstall existing third-party security software	Yes	No	No
Automatically uninstall a problem Symantec Endpoint Protection client	Yes (14)	No	No
Authentication for Symantec Endpoint Protection Manager log on	<ul style="list-style-type: none"> <li>Symantec Endpoint Protection Manager authentication</li> <li>Two-factor authentication (14.2)</li> <li>RSA SecurID authentication</li> <li>Directory authentication</li> <li>Smart card (PIV/CAC) authentication (14.2)</li> </ul>	Not applicable	Not applicable

**\*\*You can only run these commands when viewing logs in Symantec Endpoint Protection Manager.**

[What are the commands that you can run on client computers?](#)

[Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console](#)

[Monitoring the applications and services that run on client computers](#)

[Managing the client-server connection](#)

[Restoring client-server communications with Communication Update Package Deployment](#)

### AutoUpgrade differences based on platform

**Table 199: AutoUpgrade differences based on platform**

Feature	Windows	Mac
Delta package	Standard and dark network clients receive a delta upgrade package that Symantec Endpoint Protection Manager generates. Embedded clients receive the full install package for an upgrade.	Mac clients always receive a full install package for upgrade.
Configuration options	Include a custom installation folder, and the option to uninstall existing security software.	Only for restart and upgrade. You cannot customize the installation folder. Installation logging always writes to <code>/tmp/sepinstall.log</code> .

Feature	Windows	Mac
Restart options after the upgrade completes in <b>Client Install Settings</b>	Include an option to not to restart the Windows client computer.	Do not include an option to not restart. Mac client computers always restart after the upgrade completes.
<b>Upgrade Clients with Package wizard</b>	You can modify the feature set on the Windows client.	You cannot modify the feature set on the Mac client.
Upgrades from an earlier version	You can upgrade to the latest version of Symantec Endpoint Protection from any earlier version, based on the supported upgrade path.	Not supported for an upgrade from version 12.1.6.x or earlier. For example, you cannot upgrade from 12.1.6.4 to 14 using AutoUpgrade.

[Upgrading client software with AutoUpgrade](#)

[Supported upgrade paths to the latest version of Symantec Endpoint Protection 14.x](#)

[How to choose a client installation type](#)

### Virus and Spyware Protection policy settings based on platform

**Table 200: Virus and Spyware Protection policy settings based on platform**

Policy setting	Windows	Mac	Linux
Administrator-defined scans	<ul style="list-style-type: none"> <li>Scheduled scans (Active, Full, Custom)</li> <li>On-demand scans</li> <li>Triggered scans</li> <li>Startup scans</li> <li>Retry missed scheduled scans</li> <li>Randomized scheduled scans</li> </ul>	<ul style="list-style-type: none"> <li>Scheduled scans (Custom)</li> <li>On-demand scans</li> <li>Retry missed scheduled scans</li> </ul>	<ul style="list-style-type: none"> <li>Scheduled scans (Custom)</li> <li>On-demand scans</li> <li>Retry missed scheduled scans</li> </ul>
Auto-Protect	<ul style="list-style-type: none"> <li>Enable Auto-Protect</li> <li>Scan all files</li> <li>Scan only selected extensions</li> <li>Determine file types by examining file contents</li> <li>Scan for security risks</li> <li>Scan files on remote computers (14)</li> <li>Scan when files are accessed, modified, or backed up</li> <li>Scan floppies for boot viruses, with the option to delete the boot virus or log it only</li> <li>Always delete newly created infected files or security risks</li> <li>Preserve file times</li> <li>Tune scan performance for scan speed or application speed</li> <li>Emulator for packed malware (14)</li> </ul>	<ul style="list-style-type: none"> <li>Enable Auto-Protect</li> <li>Automatically repair infected files</li> <li>Quarantine files that cannot be repaired</li> <li>Scan compressed files</li> <li>Scan all files</li> <li>Scan only selected folders</li> <li>Scan everywhere except in selected folders</li> <li>Scan for security risks</li> </ul> <p><b>Scan on mount, current clients:</b></p> <ul style="list-style-type: none"> <li>Data disks</li> <li>All other disks and devices</li> </ul> <p><b>Scan on mount, legacy clients (12.1.3 and earlier):</b></p> <ul style="list-style-type: none"> <li>Music or video disks</li> <li>iPod players</li> <li>Show progress during scan</li> </ul>	<ul style="list-style-type: none"> <li>Enable Auto-Protect</li> <li>Scan all files</li> <li>Scan only selected extensions (removed in 14.3 RU1)</li> <li>Scan removable media</li> <li>Scan for security risks</li> <li>Scan files on remote computers</li> <li>Scan when files are accessed or modified</li> <li>Scan inside compressed files</li> </ul>



Policy setting	Windows	Mac	Linux
Email scans	<ul style="list-style-type: none"> <li>Microsoft Outlook Auto-Protect</li> <li>Internet email Auto-Protect (removed in 14.2 RU1)</li> <li>Lotus Notes Auto-Protect (removed in 14.2 RU1)</li> </ul>	No	No
What to scan	<ul style="list-style-type: none"> <li>Additional locations</li> <li>Memory</li> <li>Selected folders</li> <li>Selected extensions</li> <li>Storage migration locations</li> <li>Files inside compressed files</li> <li>Security risks</li> </ul>	<ul style="list-style-type: none"> <li>All or selected folders</li> <li>Hard drives and removable drives</li> <li>Files inside compressed files</li> </ul>	<ul style="list-style-type: none"> <li>All files</li> <li>All or selected folders</li> <li>Selected extensions</li> <li>Files inside compressed files</li> <li>Security risks</li> </ul>
User-defined scans (client)	<ul style="list-style-type: none"> <li>Active scan</li> <li>Full scan</li> <li>Custom scan of individual folders, files, and extensions</li> </ul>	<ul style="list-style-type: none"> <li>Full scan</li> <li>Custom scan of individual folders and files</li> </ul>	<ul style="list-style-type: none"> <li>Full scan</li> <li>Custom scan of individual folders and files</li> </ul>
Define remediation actions for detections	<ul style="list-style-type: none"> <li>Clean (only applies to malware)</li> <li>Quarantine</li> <li>Delete</li> <li>Leave alone (log only)</li> </ul> <p>The actions apply to categories of malware and security risks that Symantec periodically updates.</p>	<ul style="list-style-type: none"> <li>Repair infected files</li> <li>Quarantine files that cannot be repaired</li> </ul>	<p>(14.3 MP1 and earlier)</p> <ul style="list-style-type: none"> <li>Clean (only applies to malware)</li> <li>Quarantine</li> <li>Delete</li> <li>Leave alone (log only)</li> </ul>
Set actions to take while a scan is running	<ul style="list-style-type: none"> <li>Stop the scan</li> <li>Pause a scan</li> <li>Snooze a scan</li> <li>Scan only when the computer is idle</li> </ul>	<p>(12.1.4)</p> <ul style="list-style-type: none"> <li>Stop a scan</li> <li>Pause a scan</li> <li>Snooze a scan before it begins</li> <li>Snooze a scan that is in progress (through 12.1.6x only)</li> <li>Scan only when the computer is idle</li> </ul>	No
Download Insight	Yes	No	No
Insight lookups for threat detection	Yes	No	No
Bloodhound	Yes	No	No
SONAR	Yes Scans of remote computers (14) Suspicious Behavior Detection (14)	No	No
Early Launch Anti-Malware Driver	Windows 8 and later, and Windows Server 2012 and later	No	No
Power Eraser	Yes (12.1.5)	No	No
Endpoint Detection and Response enablement	Yes (12.1.6)	No	No

Policy setting	Windows	Mac	Linux
Shared Insight Cache	Yes vShield-enabled (12.1.6 and earlier)	No	No
Virtual Image Exception	Yes	No	No

[Preventing and handling virus and spyware attacks on client computers](#)

[Using Symantec Endpoint Protection in virtual infrastructures](#)

**Firewall, Intrusion Prevention, and Memory Exploit Mitigation, settings based on platform**

**Table 201: Intrusion Prevention policy settings based on platform**

Policy setting	Windows	Mac (12.1.4)
Exceptions for intrusion prevention signatures	Yes <b>Note:</b> Custom exceptions are not supported for Browser Protection signatures.	Yes
Show or hide user notifications	Yes	Yes
Enable or disable excluded hosts	Yes	Yes
Custom IPS signatures	Yes	No
Enable or disable Network Intrusion Prevention	Yes	Yes
LiveUpdate updates IPS content	Yes	Yes
The management server updates IPS content	Yes	No **
Client package includes IPS	Yes	Yes
Network intrusion prevention	Yes	Yes
Browser intrusion prevention	Yes • Log-only mode (12.1.6)	No
Excluded hosts (network intrusion prevention)	Yes	Yes

\*\*You can set up the Apache web server that installs with Symantec Endpoint Protection Manager as a reverse proxy for LiveUpdate content. See:

[Enabling Mac and Linux clients to download LiveUpdate content using the Apache Web server as a reverse proxy](#)

[Managing intrusion prevention](#)

**Table 202: Memory Exploit Mitigation policy settings based on platform**

Policy setting	Windows	Mac (12.1.4)
Memory Exploit Mitigation Generic Exploit Mitigation (14 MPx)	Yes (14) • Fine-tuning false positives (14.0.1) • Custom applications (14.1, cloud only)	No

[Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy](#)

---

## LiveUpdate policy settings based on platform

**Table 203: LiveUpdate policy settings based on platform**

Policy setting	Windows	Mac	Linux
Use the default management server	Yes	No **	No **
Use a LiveUpdate server (internal or external)	Yes	Yes	Yes
Use a Group Update Provider	Yes	No	No
Enable third-party content management	Yes	No	No
Enable/disable definitions	Yes	Yes	No
Reduced-size definitions (12.1.6)	Yes	No	No
Run Intelligent Updater to update content	<ul style="list-style-type: none"><li>• Virus and spyware definitions</li><li>• SONAR (12.1.3 and later)</li><li>• IPS definitions (12.1.3 and later)</li></ul>	Virus and spyware definitions	Virus and spyware definitions
LiveUpdate proxy configuration	Yes	Yes, but it is not configured in the LiveUpdate policy. To configure this setting, click <b>Clients &gt; Policies</b> , and then click <b>External Communications Settings</b> .	Yes
LiveUpdate schedule settings	<ul style="list-style-type: none"><li>• Frequency</li><li>• Retry window</li><li>• Download randomization</li><li>• Run when computer is idle</li><li>• Options for skipping LiveUpdate</li></ul>	<ul style="list-style-type: none"><li>• Frequency</li><li>• Download randomization</li></ul>	<ul style="list-style-type: none"><li>• Frequency</li><li>• Retry window</li><li>• Download randomization</li></ul>
Use standard HTTP headers (12.1.6 and earlier)	Yes, by default	Yes, by default	Yes, by default
Client security patches	Yes (14)	No	No
Application control content	Yes (14.2)	No	No

\*\* You can set up the Apache web server that installs with Symantec Endpoint Protection Manager as a reverse proxy for LiveUpdate content. See:

[Enabling Mac and Linux clients to download LiveUpdate content using the Apache Web server as a reverse proxy](#)

[How to choose a client installation type](#)

[How to update content and definitions on the clients](#)

[Using Intelligent Updater files to update content on Symantec Endpoint Protection clients](#)

## Web and Cloud Access Protection policy settings based on platform

The Integrations policy is available as of version 14.0.1 MP1. The Integrations policy was renamed to the Network Traffic Redirection policy in 14.3 RU1 and to Web and Cloud Access Protection in 14.3 RU2.

Policy setting	Windows	Mac	Linux
PAC File method <ul style="list-style-type: none"> <li>Local Proxy Service</li> </ul>	Yes	Yes <ul style="list-style-type: none"> <li>Supported for 14.2 RU2 and later.</li> </ul>	No
Tunnel method (14.3 RU1)	Yes, Windows 10 64-bit only	No	

## Configuring Web and Cloud Access Protection

### Exceptions policy settings based on platform

**Table 204: Exceptions policy settings based on platform**

Policy setting	Windows	Mac	Linux
Server-based exceptions	<ul style="list-style-type: none"> <li>Applications</li> <li>Applications to monitor</li> <li>Extensions</li> <li>Files</li> <li>Folders</li> <li>Known risks</li> <li>Trusted web domains</li> <li>Tamper Protection exceptions</li> <li>DNS or Host file change exceptions</li> <li>Certificate (14.0.1)</li> </ul>	<ul style="list-style-type: none"> <li>Security risk exceptions for files or folders</li> </ul>	<ul style="list-style-type: none"> <li>Folders</li> <li>Extensions</li> </ul>
Client restrictions (Controls which restrictions end users can add on the client computer)	Yes	No	No

## Managing exceptions in Symantec Endpoint Protection

### Device Control differences based on platform

Application control runs on Windows computers only.

**Table 205: Device Control differences based on platform**

Windows	Mac
Device control works based only on Class ID (GUID) and Device ID.	Device control works at the file system level. Volume-level tasks (such as those that can be performed via command line or Disk Utility) are unaffected.
Device control performs wildcard matches on Class ID or Device ID with the star character or asterisk (*).	Device control performs regular expression (regexp) matches, and are limited to the following specific operations: <ul style="list-style-type: none"><li>• . (dot)</li><li>• \ (backslash)</li><li>• [set], [^Set] (set)</li><li>• * (star character or asterisk)</li><li>• + (plus)</li></ul>
The Hardware Device list includes many common device types by default.	You can choose from only five device types: <ul style="list-style-type: none"><li>• Thunderbolt</li><li>• CD/DVD</li><li>• USB</li><li>• FireWire</li><li>• Secure Digital (SD) Card</li></ul> You do not use the Hardware Device list.
You can add additional custom devices to the Hardware Device list by Class ID or Device ID.	You cannot add additional custom devices.
Devices to block (or to exclude from blocking) are derived only from the Hardware Device list. The list includes those default common device types, as well as custom devices you may have added.	Devices to block (or exclude from blocking) are selected from the device types noted above. The vendor, model, and serial number can be left blank, or can be defined by regular expression (regexp) queries. You can use regular expressions to define a range of similar devices, such as from different vendors, model, serial number ranges, and so on.
You can add more than one device type at a time.	You can only add one device type at a time.
The actions to take are to block, or to exclude from blocking (allow).	The actions to take are to block, or to exclude from blocking (allow) with mount permissions. The following mount permissions are supported: <ul style="list-style-type: none"><li>• Read only</li><li>• Read and write</li><li>• Read and execute</li><li>• Read, write, and execute</li></ul>
You can customize the client notification for device control.	You cannot customize the client notifications for device control.

### Managing device control

## Symantec Endpoint Protection feature dependencies for Windows clients

Some policy features require each other to provide complete protection on Windows client computers.

### WARNING

Symantec recommends that you do not disable Insight lookups.

**Table 206: Dependencies of protection features**

Feature	Interoperability Notes
Download Protection	<p>Download Protection is part of Auto-Protect and gives Symantec Endpoint Protection the ability to track URLs. The URL tracking is required for several policy features.</p> <p>If you install Symantec Endpoint Protection without Download Protection, Download Insight has limited capability. Browser Intrusion Prevention and SONAR require Download Protection.</p> <p>The <b>Automatically trust any file downloaded from an intranet website</b> option also requires Download Protection.</p>
Download Insight	<p><b>Download Insight has the following dependencies:</b></p> <ul style="list-style-type: none"> <li>• Auto-Protect must be enabled If you disable Auto-Protect, Download Insight cannot function even if Download Insight is enabled.</li> <li>• Insight lookups must be enabled Symantec recommends that you keep the Insight lookups option enabled. If you disable the option, you disable Download Insight completely.</li> </ul> <p><b>Note:</b> If basic Download Protection is not installed, Download Insight runs on the client at level 1. Any level that you set in the policy is not applied. The user also cannot adjust the sensitivity level.</p> <p>Even if you disable Download Insight, the <b>Automatically trust any file downloaded from an intranet website</b> option continues to function.</p> <p>If you disable Download Insight, you disable portal detections. This means that Auto-Protect and scheduled and on-demand scans evaluate all files as non-portal files and use a sensitivity level that is determined by Symantec.</p> <p><a href="#">Managing Download Insight detections</a></p>
Insight Lookup (12.1.x clients) and cloud protection	<p>Insight Lookup uses the Symantec Insight reputation database in the cloud to make decisions about files that were downloaded from a supported portal.</p> <p><b>Starting in 14:</b></p> <ul style="list-style-type: none"> <li>• The Insight Lookup functionality runs automatically as part of Auto-Protect, scheduled scans, and on-demand scans on standard and embedded/VDI clients. The standard and embedded/VDI clients support cloud-enabled content.</li> <li>• You can enable or disable Insight Lookup in the scan settings for any 12.1.x clients you have, but you can no longer configure a specific sensitivity level for Insight Lookup. Legacy Insight Lookup now uses the sensitivity level that is set in the Download Insight policy.</li> </ul> <p><a href="#">How Windows clients receive definitions from the cloud</a></p> <p>Cloud scans and 12.1.x Insight Lookup have the following feature dependencies:</p> <ul style="list-style-type: none"> <li>• Insight lookups must be enabled. Otherwise, cloud scans and Insight Lookup cannot function.</li> <li>• Download Insight must be enabled so that files can be marked as portal files.</li> <li>• If Download Insight is disabled, cloud scans and Insight Lookup continue to function. They use a sensitivity level that is automatically set by Symantec that detects only the most malicious files.</li> </ul> <p><b>Note:</b> (12.1.x clients only) Cloud lookups do not apply to right-click scans of folders or drives on your client computers. However, cloud lookups do apply to right-click scans of selected portal files.</p>

Feature	Interoperability Notes
SONAR	<p><b>SONAR has the following dependencies:</b></p> <ul style="list-style-type: none"> <li>Download Protection must be installed.</li> <li>Auto-Protect must be enabled.</li> </ul> <p>If Auto-Protect is disabled, SONAR loses some detection functionality and appears to malfunction on the client. SONAR can detect heuristic threats, however, even if Auto-Protect is disabled.</p> <ul style="list-style-type: none"> <li>Insight lookups must be enabled.</li> </ul> <p>Without Insight lookups, SONAR can run but cannot make detections. In some rare cases, SONAR can make detections without Insight lookups. If Symantec Endpoint Protection has previously cached reputation information about particular files, SONAR might use the cached information.</p> <p><a href="#">Managing SONAR</a></p>
Browser Intrusion Prevention	Download Protection must be installed. Download Insight can be enabled or disabled.
Trusted Web Domain exception	The exception is only applied if Download Protection is installed.
Custom IPS signatures	<p>Uses the firewall.</p> <p><a href="#">Managing custom intrusion prevention signatures</a></p>
Power Eraser	<p>Uses Insight lookups.</p> <p>Power Eraser uses reputation information to examine files. Power Eraser has a default reputation sensitivity setting that you cannot modify. If you disable the option <b>Allow Insight lookups for threat detection</b>, Power Eraser cannot use reputation information from Symantec Insight. Without Insight, Power Eraser makes fewer detections, and the detections are more likely to be false positives.</p> <p><b>Note:</b> Power Eraser uses its own reputation thresholds that are not configurable in Symantec Endpoint Protection Manager. Power Eraser does not use the Download Insight settings.</p> <p><a href="#">What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console</a></p>
Memory Exploit Mitigation (Generic Exploit Mitigation in version 14)	Intrusion prevention must be installed. Intrusion prevention can be enabled or disabled.

[Choosing which security features to install on the client](#)

## What are the tools included with Symantec Endpoint Protection?

This article describes the tools that are included with Symantec Endpoint Protection and what you use the tools for.

[Tools that are located on the installation file on FileConnect](#)

[Tools that are installed with Symantec Endpoint Protection Manager](#)

### Tools that are located on the installation file

The following tools and documentation are located in the \Tools folder of the Symantec Endpoint Protection installation file that you download from the Broadcom [Download Management](#) page.

- 
- [ApacheReverseProxy \(12.1.4 and later\)](#)
  - [CentralQ \(12.1.6 and earlier\)](#)
  - [CleanWipe](#)
  - [ContentDistributionMonitor \(SEPMMonitor\)](#)
  - [Deception \(14.0.1\)](#)
  - [DeviceInfo \(14\), DevViewer](#)
  - [Integration \(WebServicesDocumentation\)](#)
  - [ITAnalytics](#)
  - [JAWS](#)
  - [LiveUpdate Administrator \(12.1.4 and earlier\)](#)
  - [No Support > MoveClient](#)
  - [No Support > Qextract](#)
  - [No Support > SEPprep \(12.1.6 and earlier\)](#)
  - [OfflineImageScanner \(12.1.6 and earlier\)](#)
  - [PushDeploymentWizard](#)
  - [SylinkDrop](#)
  - [SymDiag \(SymHelp\)](#)
  - [Virtualization](#)
  - [WebServicesDocumentation \(Integration\)](#)

[Product guides for all versions of Symantec Endpoint Protection](#)

### **ApacheReverseProxy (12.1.4 and later)**

This tool sets up the Apache webserver in Symantec Endpoint Protection Manager to allow Mac clients and Linux clients to download LiveUpdate content through the web server. The Apache webserver works with the Symantec Endpoint Protection Manager to download and cache the LiveUpdate content for Mac and Linux clients locally whenever new content is published.

This tool is appropriate for networks with a smaller number of clients.

### **CentralQ (12.1.6 and earlier)**

Symantec Endpoint Protection can automatically forward the quarantine packages that contain the infected files and related side effects from a local quarantine to the Central Quarantine. You can gather forensic information more easily by using Central Quarantine. This tool lets you retrieve a sample from an infected computer without having to directly access that computer.

Use the Quarantine Server in a Symantec Endpoint Protection environment in the following cases:

- To receive suspected threat samples from Symantec Endpoint Protection clients.
- To submit these samples to Security Response automatically.
- To download the rapid release definitions that are specific to the suspected threats that have been submitted only to the Quarantine Server. These definitions are not pushed to the Symantec Endpoint Protection clients where the threat originated from.

[Rapid Release Virus Definitions](#)

For more information, see: [Best Practices for using Quarantine Server in a Symantec Endpoint Protection environment](#)

### **CleanWipe**

CleanWipe uninstalls the Symantec Endpoint Protection product. Only use CleanWipe as a last resort after you have unsuccessfully tried other uninstallation methods, such as the Windows Control Panel.

[Uninstall Symantec Endpoint Protection](#)



---

You can also find this tool in the following location (64-bit): C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

### **ContentDistributionMonitor (SEPMMonitor)**

The ContentDistributionMonitor tool helps you manage and monitor multiple Group Update Providers (GUPs) in your environment. The tool presents a graphical display of the GUPs' health and content distribution status.

In 12.1.6 and earlier, ContentDistributionMonitor was named SEPMMonitor. In 12.1.5 and earlier, ContentDistributionMonitor was in the NoSupport folder.

See: [Symantec Endpoint Protection Content Distribution Monitor tool](#)

### **Deception (14.0.1)**

Deception is used to detect adversary activity at the endpoint using "deceptors." The underlying assumption with this approach is that the attacker has already breached the primary defenses of the network and performs reconnaissance in the environment. The attacker looks to find critical assets, like a domain controller or database credentials.

### **DeviceInfo (14), DevViewer**

DeviceInfo (for Mac; as of version 14) and DevViewer (for Windows) obtains the device vendor, model, or serial number for a specific device. You add this information to the **Hardware Devices** list. You can then add the device ID to a Device Control policy to allow or block a device on client computers.

Download DevViewer from the Attachments section at: [Use DevViewer to find hardware device IDs for Device Blocking in Endpoint Protection](#)

[Adding a hardware device to the Hardware Devices list](#)

[Block or allow devices in Endpoint Protection](#)

### **Integration (WebServicesDocumentation)**

As of version 14, the Integration folder was renamed to WebServicesDocumentation.

[Adding a hardware device to the Hardware Devices list](#)

### **ITAnalytics**

The IT Analytics software expands the built-in reporting that Symantec Endpoint Protection offers by enabling you to create custom reports and custom queries. It brings multi-dimensional analysis and graphical reporting features from the data that is contained within the Symantec Endpoint Protection Manager databases. This functionality allows you to explore data on your own, without advanced knowledge of databases or third-party reporting tools.

### **JAWS**

The JAWS screen reader program and a set of scripts make it easier to read the Symantec Endpoint Protection menus and dialogs. JAWS is an assistive technology that provides compliance with Section 508 product accessibility.

### **LiveUpdate Administrator (12.1.4 and earlier)**

Symantec LiveUpdate Administrator is a standalone web application that is separate from Symantec Endpoint Protection. LiveUpdate Administrator mirrors the content of the public LiveUpdate servers and then offers the content to Symantec products internally through a built-in web server.

LiveUpdate Administrator is an optional component for Symantec Endpoint Protection and is not required to update the Symantec Endpoint Protection clients. By default, the Symantec Endpoint Protection Manager uses the LiveUpdate technology rather than LiveUpdate Administrator to download contents directly from the Symantec public LiveUpdate servers.

You may want to use LiveUpdate Administrator in some circumstances. For example, you may need to download content to a large number of non-Windows clients or to clients if Symantec Endpoint Protection Manager cannot download

---

the content. Therefore, you can install a LiveUpdate Administrator server and then configure the Symantec Endpoint Protection Manager to download from it.

#### [When to use LiveUpdate Administrator](#)

To download LiveUpdate Administrator and the documentation, see: [Download LiveUpdate Administrator \(LUA\)](#)

#### [LiveUpdate Administrator 2.3.x Release Notes](#)

#### **No Support > MoveClient**

`MoveClient` is a Visual Basic script that moves clients from one Symantec Endpoint Protection Manager group to another group based on the client's host name, user name, IP address, or operating system. It also can switch clients from user mode to computer mode and vice versa.

#### [Switching a Windows client between user mode and computer mode](#)

#### **No Support > Qextract**

`Qextract` extracts and restores files from the client's local quarantine. You might need this tool if the client quarantines a file that you determine is a false positive.

#### **No Support > SEPprep (12.1.6 and earlier)**

SEPprep is an unsupported tool that uninstalls competitors' antivirus products automatically. SEPprep also uninstalls Symantec Norton™ products if you want to migrate from Norton to Symantec Endpoint Protection.

You can package SEPprep in a script which uninstalls the competitor's product, and then launches the Symantec Endpoint Protection installer automatically and silently.

Instead of SEPprep, use the Client Deployment Wizard to uninstall competitors' products. On the **Client Install Settings** tab in the wizard, click **Automatically uninstall existing third-party security software**.

#### [Configuring client packages to uninstall existing security software](#)

#### [Uninstall third-party security software using SEPprep](#)

For a list of products that the Client Deployment Wizard uninstalls, see:

#### [Third-party security software removal in Endpoint Protection 12.1](#)

SEPprep does not uninstall any Symantec products. However, as of version 14, CleanWipe is built into the Client Deployment Wizard to remove other Symantec products, including the Symantec Endpoint Protection client.

#### **OfflineImageScanner (12.1.6 and earlier)**

This tool scans and detects threats in offline VMware virtual disks (.vmdk files).

#### [About the Symantec Offline Image Scanner tool](#)

#### **PushDeploymentWizard**

You use the Push Deployment Wizard to deploy the Symantec Endpoint Protection client installation package to target computers. Push Deployment Wizard is the same as the Client Deployment Wizard in Symantec Endpoint Protection Manager. You typically use it to deploy to smaller groups of computers or remote computers.

For more information, see: [Overview of the Push Deployment Wizard in Symantec Endpoint Protection](#)

#### **SEPIIntegrationComponent (12.1.5 and earlier)**

The Symantec Endpoint Integration Component (SEPIC) combines Symantec Endpoint Protection with other Symantec Management Platform solutions using a single, web-based Symantec Management Console. You use SEPIC to inventory computers, update patches, deliver software, and deploy new computers. You can also back up and restore your systems and data, manage DLP agents, and manage Symantec Endpoint Protection clients.

#### **SylinkDrop**

---

The Sylink.xml file includes communication settings between the Windows client or Mac client and a Symantec Endpoint Protection Manager. If the clients have lost the communication with Symantec Endpoint Protection Manager, use the SylinkDrop tool to automatically replace the existing Sylink.xml file with a new Sylink.xml file on the client computer.

Replacing the Sylink.xml file does the following tasks:

- Converts an unmanaged client to a managed client.
- Migrates or moves clients to a new domain or management server.
- Restores the communication breakages to the client that cannot be corrected on the management server.
- Moves a client from one server to another server that is not a replication partner.
- Moves a client from one domain to another.

You can also use this tool for Windows clients only; the tool is located in the following location (64-bit): C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

[Restoring client-server communication settings by using the SylinkDrop tool](#)

### **SymDiag (SymHelp)**

As of version 14, the SymHelp tool was renamed as Symantec Diagnostic (SymDiag).

SymDiag is a multi-product diagnostic tool that identifies common issues, gathers data for support-assisted troubleshooting, and provides links to other customer self-help and support resources. SymDiag also provides licensing and maintenance status for some Symantec products as well as the Threat Analysis Scan, which helps to find potential malware.

### **Virtualization**

The virtualization tools improve scan performance for the clients that are installed in virtual desktop infrastructure (VDI) environments.

- **SecurityVirtualAppliance (12.1.6 and earlier)**

The Symantec Security Virtual Appliance contains the vShield-enabled Shared Insight Cache for VMware vShield infrastructures.

[What do I need to do to install a Security Virtual Appliance?](#)

[Installing a Symantec Endpoint Protection Security Virtual Appliance](#)

- **SharedInsightCache**

The Shared Insight Cache tool improves scan performance in virtualized environments by not scanning the files that a Symantec Endpoint Protection client has determined are clean. When the client scans a file for threats and determines it is clean, the client submits information about the file to Shared Insight Cache.

When another client subsequently attempts to scan the same file, that client can query Shared Insight Cache to determine if the file is clean. If the file is clean, the client does not scan that particular file. If the file is not clean, the client scans the file for viruses and submits those results to Shared Insight Cache.

Shared Insight Cache is a web service that runs independently of the client. However, Symantec Endpoint Protection must be configured to specify the location of Shared Insight Cache so that the clients can communicate with it. Shared Insight Cache communicates with the clients through HTTP or HTTPS. The client's HTTP connection is maintained until the scan is finished.

[Installation and Configuration of SEP Shared Insight Cache](#)

- **Virtual Image Exception**

To increase performance and security in a VDI environment, a common practice is to leverage base images to build virtual machine sessions as needed. The Symantec Virtual Image Exception tool lets Symantec Endpoint Protection clients bypass scanning base image files for threats, which reduces the resource load on disk I/O. It also improves CPU scanning process performance in a VDI environment.

[About the Symantec Virtual Image Exception tool](#)

### **WebServicesDocumentation (Integration)**

---

In 12.1.6 and earlier, this tool is located in the \Tools\Integration folder.

Symantec Endpoint Protection includes a set of public APIs in the form of web services to provide support for remote monitoring and management (RMM) applications. The web services provide functions on the client and on the management server. All calls to Symantec Endpoint Protection web services are authenticated using OAuth and allow access only by authorized Symantec Endpoint Protection administrators. Developers use these APIs to integrate their company's third-party network security solution with the Symantec Endpoint Protection management server and client.

Provides the support for remote management and remote monitoring. Remote management is provided by means of public APIs in the form of web services that let you integrate your third-party solution or custom console with basic client and management server functionality. Remote monitoring is provided by means of publicly supported registry keys and Windows event logging.

**Web services for remote management can do the following tasks:**

- Reports the license status and content status on the management server by web service calls, in addition to reporting the license status to the Windows Event Log.
- Issues commands to the client, such as Update, Update and Scan, and Restart.
- Manages the policies that are delivered to the client. Policies can be imported from another management server, and they can be assigned to groups or locations at another management server.

**Tools that are installed with Symantec Endpoint Protection Manager**

The following tools are installed with the Symantec Endpoint Protection Manager in the following default location: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools.

- [CleanWipe](#)
- [CollectLog](#)
- [Database Validator](#)
- [SetSQLServerTLSEncryption](#)
- [SylinkDrop](#)
- [Symantec Endpoint Protection Manager API reference](#)

**CollectLog**

CollectLog.cmd places the Symantec Endpoint Protection Manager logs in a compressed .zip file. You send the .zip file to Symantec Support or another administrator for troubleshooting purposes.

You find this tool in the following location (64-bit): C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

**Database Validator**

You use dbvalidator.bat to help Support diagnose a problem with the database that Symantec Endpoint Protection Manager runs.

You find this tool in the following location (64-bit): C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

**SetSQLServerTLSEncryption (14)**

Symantec Endpoint Protection Manager communicates with the Microsoft SQL Server over an encrypted channel by default. This tool lets you disable or enable TLS encryption between the management server and the Microsoft SQL Server communication. As of version 14, it can be used with the management server installations that are configured to use the Microsoft SQL Server database.

This tool is installed with Symantec Endpoint Protection Manager in the following location (64-bit): C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

**Symantec Endpoint Protection Manager API reference (14)**

Symantec Endpoint Protection Manager includes a set of REST APIs that connect to and perform Symantec Endpoint Protection Manager operations from Endpoint Detection and Response (EDR). You use the APIs if you do not have access to Symantec Endpoint Protection Manager. The documentation is located in the following places:

- On the Symantec Endpoint Protection Manager server at the following address, where SEPM-IP is the IP address of the Symantec Endpoint Protection Manager server:  
`https://SEPM-IP:8446/sepm/restapidocs.html`  
IP address includes IPv4 and IPv6. You must enclose the IPv6 address with square brackets: `http://[SEPMServer]:port number`
- [Product guides for all versions of Symantec Endpoint Protection](#)

## Commands for the Windows client service smc in Symantec Endpoint Protection and Symantec Endpoint Security

You can run the Windows client service using the `smc` (or `smc.exe`) command-line interface. You can use the `smc` command in a script that runs the client remotely. For example, you may need to stop the client to install an application on multiple clients. You can then use the script to stop and restart all clients at one time.

The client service must be running for you to use the command-line parameters, with the exception of `smc -start` parameter. The command-line parameters are not case-sensitive. For some parameters, you may need the password. The client does not support UNC paths.

To run Windows commands using the `smc` command-line interface:

1. On the client computer, click **Start > Run**, and then type `cmd`.
  2. In the Command Prompt window, do one of the following tasks:
    - If the parameter does not need a password, enter:  
`smc -parameter`  
Where parameter is a parameter.
    - If the parameter needs a password, enter:
      - `smc -p password -parameter`
- For example: `smc -p password -exportconfig c:\profile.xml`

### NOTE

You must enter the installation path to the `smc` service before the command. For example, on a 64-bit Windows system on which Symantec Endpoint Protection is installed to the default location, enter:

```
C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\smc.exe
```

**Table 207: Parameters for smc**

Parameter	Description	Applies to
<code>smc -start *</code>	Starts the client service. Returns 0, -1	All supported versions
<code>smc -stop *†</code>	Stops the client service and unloads it from memory. If this command is password-protected, the client is disabled within one minute after the end user enters the correct password. Returns 0, -1	All supported versions

Parameter	Description	Applies to
smc -cloudmanaged path\to \Symantec_Agent_Setup.exe	<p>Moves a cloud-managed device to another cloud domain or tenant.</p> <p>Moves a client computer from Symantec Endpoint Protection Manager management to cloud console management.</p> <p>Requires the Symantec_Agent_Setup.exe installation file for the destination cloud domain or tenant. You download this file from the cloud console.</p> <p><a href="#">Using smc to change a device's tenant or domain</a></p>	As of 14.2 RU1
smc -enable -ntp smc -disable -ntp †	Enables/disables the Symantec Endpoint Protection firewall and Intrusion Prevention System.	All supported versions Password requirement for -disable as of 14.2 RU1
smc -enable -mem * smc -disable -mem *	Enables/disables the Symantec Endpoint Protection Memory Exploit Mitigation system.	As of version 14 MP1
Version 14: smc -enable -gem * Version 14: smc -disable -gem *	<p>Enables/disables the Symantec Endpoint Protection Generic Memory Exploit Mitigation system.</p> <p>This feature is called Memory Exploit Mitigation in subsequent versions.</p>	Version 14 only
smc -dismissgui	<p>Closes the client user interface.</p> <p>The client still runs and protects the client computer.</p> <p>Returns 0</p>	All supported versions
smc -exportconfig *†	<p>Exports the client's configuration file to an .xml file. The configuration file includes the following management server settings:</p> <ul style="list-style-type: none"> <li>• Policies</li> <li>• Groups</li> <li>• Security settings</li> <li>• User interface settings</li> </ul> <p>You must specify the path name and file name. For example, you can enter the following command:</p> <pre>smc -exportconfig C:\My Documents\MyCompanyprofile.xml</pre> <p>Returns 0, -1, -5, -6</p>	All supported versions
smc -exportlog	<p>Exports the entire contents of a log to a .txt file.</p> <p>To export a log, you use the following syntax:</p> <pre>smc -exportlog log_type 0 -1 output_file</pre> <p>Where:</p> <p>log_type is:</p> <ul style="list-style-type: none"> <li>• 0 = System Log</li> <li>• 1 = Security Log</li> <li>• 2 = Traffic Log</li> <li>• 3 = Packet Log</li> <li>• 4 = Control Log</li> </ul> <p>For example, you might enter the following syntax:</p> <pre>smc -exportlog 2 0 -1 c:\temp\TrafficLog</pre> <p>Where 0 is the beginning of the file and -1 is the end of the file.</p> <p>You can export only the Control log, Packet log, Security log, System log, and Traffic log.</p> <p>The name output_file is the path name and file name that you assign to the exported file.</p> <p>Returns 0, -2, -5</p>	All supported versions

Parameter	Description	Applies to
<code>smc -exportadvrule *†</code>	<p>Exports the client's firewall rules to an .xml file. The exported rules can only be imported into an unmanaged client or a managed client in client control mode or mixed mode. The managed client ignores these rules in server control mode.</p> <p>You must specify the path name and file name. For example, you can enter the following command:</p> <pre>smc -exportadvrule C:\myrules.xml</pre> <p>Returns 0, -1, -5, -6</p> <p>When you import configuration files and firewall rules, note that the following rule applies:</p> <ul style="list-style-type: none"> <li>You cannot import configuration files or firewall rule files directly from a mapped network drive.</li> </ul>	All supported versions
<code>smc -importadvrule *†</code>	<p>Imports the firewall rules to the client. The rules you import overwrite any existing rules. You can import the following:</p> <ul style="list-style-type: none"> <li>Rules in .xml format that you exported through <code>smc -exportadvrule</code></li> <li>Rules in .sar format that you exported through the client user interface</li> </ul> <p>You can only import firewall rules if the client is unmanaged or if the managed client is in client control mode or mixed mode. The managed client ignores these rules in server control mode.</p> <p>To import firewall rules, you import an .xml or .sar file. For example, you can enter the following command:</p> <pre>smc -importadvrule C:\myrules.xml</pre> <p>An entry is added to the System log after you import the rules.</p> <p>Returns 0, -1, -5, -6</p> <p>To append rules instead of overwriting them, use <b>Import rule</b> from the within client user interface.</p> <p><a href="#">Preventing and allowing users to change the client's user interface</a></p> <p><a href="#">Exporting or importing firewall rules on the client</a></p>	All supported versions
<code>smc -importconfig *†</code>	<p>Replaces the contents of the client's current configuration file with an imported configuration file and updates the client's policy. The client must run to import the configuration file's contents.</p> <p>You must specify the path name and file name. For example, you can enter the following command:</p> <pre>smc -importconfig C:\My Documents\MyCompanyprofile.xml.</pre> <p>Returns 0, 3, -1, -5, -6</p>	All supported versions
<code>smc -importsymlink path \to\symlink.xml †</code>	<p>Imports the client communications file (symlink.xml).</p> <p>Equivalent to <code>-sepmmanaged</code>.</p>	All supported versions
<code>smc -enable -wss</code> <code>smc -disable -wss</code>	Enables or disables Web and Cloud Access Protection.	As of version 14.0.1 MP1
<code>smc -p password †</code>	<p>Used with a command that requires a password, where password is the required password. For example:</p> <pre>smc -p password -importconfig</pre>	All supported versions
<code>smc -report</code>	<p>Creates a dump file (.dmp) that includes crashes and logical errors that occurred on the client. The file is sent automatically to Symantec Technical Support. Contact Technical Support to ask for help in diagnosing the error.</p> <p>You can find the dump file at the following location:</p> <pre>SEP_Install\Data\LocalDumps</pre> <p>Where SEP_Install is the installation folder. By default, this path is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\version.</p>	As of version 14



Parameter	Description	Applies to
<code>smc -runhi</code>	Runs a Host Integrity check. Returns 0	All supported versions
<code>smc -sepmmanaged</code>	Reverts the client management from the cloud console back to the Symantec Endpoint Protection Manager that previously managed it.	As of 14.2 RU1
<code>smc -sepmmanaged path \to\sylink.xml</code>	Updates the client management to the Symantec Endpoint Protection Manager specified in the SyLink.xml file. Equivalent to <code>-importsylink</code> .	As of 14.2 RU1
<code>smc -showgui</code>	Displays the client user interface. Returns 0	All supported versions
<code>smc -updateconfig</code>	Initiates a client-server communication to ensure that the client's configuration file is up-to-date. If the client's configuration file is out-of-date, <code>updateconfig</code> downloads the most recent configuration file and replaces the existing configuration file, which is <code>serdef.dat</code> . Returns 0	All supported versions
<code>smc -image</code>	Unenrolls the Symantec Agent (Symantec Endpoint Protection client) and keeps it unenrolled. The difference from a regular unenrollment is the removal of the hardware key and the persisted hardware key information.	As of 14.3 RU1 (Symantec Endpoint Security only)
<code>smc -configure -customer-id &lt;id&gt; -domain-id &lt;id&gt; -customer-secret-key &lt;cc token&gt; -server-address &lt;full bootstrap URL&gt;</code>	Enrolls a device and uses existing proxy options from the device. All enrollment parameters are required.	As of 14.3 RU1
<code>smc -configure -proxy-mode &lt;mode&gt;</code>	Used together with enrollment parameters to enable the client to enroll using the required proxy configuration. Can also be used to correct bad proxy options. Possible modes are as follows: <b>system</b> , <b>manual</b> , <b>none</b> . Specifying a proxy address switches automatically to <b>manual</b> mode. If you enter <b>manual</b> , but don't specify a proxy host, this mode will be ignored. Not supported on the clients that are managed by Symantec Endpoint Protection Manager. <a href="#">Combinations of proxy settings</a>	As of 14.3 RU1
<code>smc -configure -proxy-address &lt;host or IP&gt;</code>	Allows to manually specify the proxy host or the proxy address. Required if the proxy mode is set to <b>manual</b> .	As of 14.3 RU1
<code>smc -configure -proxy-port &lt;port number&gt;</code>	Allows to manually specify the proxy port. The same port will be used both for HTTP and HTTPS connections. If no ports are specified, the ports are automatically set to 80 for HTTP and 443 for HTTPS.	As of 14.3 RU1
<code>smc -configure -proxy-port-http &lt;port number&gt;</code>	Allows to manually specify the proxy port for HTTP connections. Overwrites the default HTTP port or the port that has been specified by <code>smc -configure -proxy-port</code> .	As of 14.3 RU1
<code>smc -configure -proxy-port-https &lt;port number&gt;</code>	Allows to manually specify the proxy port for HTTPS connections. Overwrites the default HTTPS port or the port that has been specified by <code>smc -configure -proxy-port</code> .	As of 14.3 RU1
<code>smc -configure -proxy-auth-mode basic</code>	Possible authentication modes are as follows: <b>basic</b> , <b>ntlm</b> . Default authentication mode is <b>basic</b> .	As of 14.3 RU1



Parameter	Description	Applies to
<code>smc.exe -configure -proxy-user-name &lt;name&gt;</code>	Allows to manually specify the proxy user. For <b>ntlm</b> , you must specify domain/user.	As of 14.3 RU1
<code>smc -configure -proxy-password &lt;plain pwd&gt;</code>	Allows to manually specify the proxy password. Maximum length is 255 characters without null. The password is case sensitive.	As of 14.3 RU1
<code>smc -reset-state -configure -customer-id &lt;epmp id&gt; -domain-id &lt;epmp id&gt; -server-address &lt;bootstrap URL&gt;</code>	Unenrolls the client and then enrolls it again as a new device. All required -configure enrollment options must be provided.	As of 14.3 RU1
<code>smc -tags "&lt;csv alphanumeric strings&gt;"</code>	Allows to manually specify the enrollment tags. Maximum length is 1024 characters without null. Must be specified together with enrollment parameters.	As of 14.3 RU1

`smc -checkinstallation` and `smc -checkrunning` are no longer supported.

\* Parameters that only members of the Administrators group can use if the following conditions are met:

- The client runs Windows Vista or Windows Server 2008, and users are members of the Windows Administrators group.  
If the client runs Windows Vista, and User Account Control is enabled, the user automatically becomes a member of the groups Administrators and Users.

† Parameters that need a password. You password-protect the client in Symantec Endpoint Protection Manager.

**Table 208: Combinations of proxy settings entered at a command prompt**

Combinations of proxy settings					Action
proxy-mode	proxy-user-name	proxy-password	proxy-address	proxy-port	
<b>system</b>	no	no	no	no	Use system proxy
<b>system</b>	<b>yes</b>	no	no	no	ERROR_INVALID_COMMAND_LINE (missing password)
<b>system</b>	no	<b>yes</b>	no	no	ERROR_INVALID_COMMAND_LINE (missing user)
<b>system</b>	no	no	<b>yes</b>	no	Use system proxy (ignore server)
<b>system</b>	<b>yes</b>	<b>yes</b>	no	no	Use system proxy with authentication
<b>system</b>	<b>yes</b>	<b>yes</b>	<b>yes</b>	no	Use system proxy with authentication (ignore server)
<b>system</b>	<b>yes</b>	<b>yes</b>	<b>yes</b>	<b>yes</b>	Use system proxy with authentication (ignore server and ports)
<b>manual</b>	no	no	no	no	ERROR_INVALID_COMMAND_LINE
<b>manual</b>	<b>yes</b>	no	no	no	ERROR_INVALID_COMMAND_LINE
<b>manual</b>	no	<b>yes</b>	no	no	ERROR_INVALID_COMMAND_LINE
<b>manual</b>	no	no	<b>yes</b>	no	Valid "manual" (custom) proxy with default ports

Combinations of proxy settings					Action
proxy-mode	proxy-user-name	proxy-password	proxy-address	proxy-port	
manual	yes	yes	no	no	ERROR_INVALID_COMMAND_LINE
manual	yes	yes	yes	no	Valid "manual" (custom) proxy with default ports
manual	yes	yes	yes	yes	Valid "manual" (custom) proxy
manual	yes	no	yes	yes or no	ERROR_INVALID_COMMAND_LINE (no password)
manual	no	yes	yes	yes or no	ERROR_INVALID_COMMAND_LINE (no user)
none	no	no	no	no	Valid "none" proxy
none	yes	no	no	no	Valid "none" proxy
none	no	yes	no	no	Valid "none" proxy
none	no	no	yes	no	Valid "none" proxy
none	yes	yes	no	no	Valid "none" proxy
none	yes	yes	yes	no	Valid "none" proxy
none	yes	yes	yes	yes	Valid "none" proxy
no	no	no	no	no	No proxy settings
no	yes	no	no	no	No proxy settings (ignore user)
no	no	yes	no	no	No proxy settings (ignore password)
no	no	no	yes	no	Valid "manual" (custom) proxy with default ports
no	yes	yes	no	no	No proxy settings (ignore extra options)
no	yes	yes	yes	no	Valid "manual" (custom) proxy with default ports
no	yes	yes	yes	yes	Valid "manual" (custom) proxy

[command error codes](#)

## smc.exe command error codes

[command error codes](#) displays the error codes that the `smc.exe` command returns when the required parameters are invalid or missing.

**Table 209: smc.exe command error codes**

Error code	Description
0	Command was successful.
-1	User is not in the Windows Administrators or Windows Power Users group. If the client runs Windows Vista, the user is not a member of the Windows Administrators group.
-2	Invalid parameter. You may have typed the parameter incorrectly, or you may have added an incorrect switch after the parameter.

Error code	Description
-3	smc client service is not installed.
-4	smc client service is not running.
-5	Invalid input file. For example, the <code>importconfig</code> , <code>exportconfig</code> , <code>updateconfig</code> , <code>importadv</code> , <code>exportadvrule</code> , and <code>exportlog</code> parameters require the correct path name and file name.
-6	Input file does not exist. For example, the <code>importconfig</code> , <code>updateconfig</code> , and <code>importadvrule</code> parameters require the correct path name, configuration file name (.xml) or firewall rules file name (.sar).

[Windows commands for the Endpoint Protection client service](#)

## Installing Windows client software using third-party tools

You can install the client using third-party tools instead of the tools that are installed with the management server. If you have a large network, you are more likely to benefit by using these options to install Symantec client software.

You can install the client by using a variety of third-party products. These products include Microsoft Active Directory, Tivoli, Microsoft Systems Management Server (SMS), and Novell ZENworks. Symantec Endpoint Protection supports Novell ZENworks, Microsoft Active Directory, and Microsoft SMS.

You can also deploy Symantec Endpoint Protection in an environment that you manage with a **Symantec Software Management Solution powered by Altiris**. You can deploy Symantec Endpoint Protection from one of the Software Management Solution suites with one of the following policies:

- A **Managed Software Delivery** policy
- A **Quick Delivery** policy

For more information, refer to the Software Management Solution suite product Help, or see:

[Symantec Software Management Solution product landing page](#)

**Table 210: Third-party tools to install the client**

Tool	Description
Windows Installer command-line tools	<p>The Symantec client software installation packages are Windows Installer (MSI) files that you can configure by using the standard Windows Installer options. You can use the environment management tools that support MSI deployment, such as Active Directory or Tivoli, to install clients on your network. You can configure how the Windows Security Center interacts with the unmanaged client.</p> <p><a href="#">About client installation features and properties</a></p> <p><a href="#">About configuring MSI command strings</a></p> <p><a href="#">About configuring Setaid.ini</a></p> <p><a href="#">Symantec Endpoint Protection command-line client features</a></p> <p><a href="#">Symantec Endpoint Protection command-line client installation properties</a></p> <p><a href="#">Windows Installer parameters</a></p> <p><a href="#">Command-line examples for installing the Windows client</a></p> <p><a href="#">Windows Security Center properties</a></p>
Microsoft SMS 2003	<p>You can install the client by using Microsoft Systems Management Server.</p> <p><a href="#">Installing Windows clients with Microsoft SCCM/SMS</a></p>

Tool	Description
Windows Active Directory	You can use a Windows Active Directory Group Policy Object if the client computers are members of a Windows Active Directory domain. The client computers must also use a supported Windows operating system. <a href="#">Installing Windows clients with an Active Directory Group Policy Object (GPO)</a> <a href="#">Uninstalling client software with an Active Directory Group Policy Object</a>
Virtualization software	You can install the client in virtual environments. <a href="#">Supported virtual installations and virtualization products</a>

[Exporting client installation packages](#)

## About client installation features and properties

Installation features and properties appear as strings in text files and command lines. Text files and command lines are processed during all client software installations. Installation features control which components get installed. Installation properties control which subcomponents are enabled or disabled after installation. Installation features and properties are available for Symantec Endpoint Protection client software only and are also available for the Windows operating system. Installation features and properties are not available for the installation of Symantec Endpoint Protection Manager.

Installation features and properties are specified in the following ways: as lines in the Setaid.ini file and as values in Windows Installer (MSI) commands. MSI commands can be specified in Windows Installer strings and in Setaid.ini for a customized deployment. Windows Installer commands and Setaid.ini are always processed for all managed client software installations. If different values are specified, the values in Setaid.ini always take precedence.

## About configuring MSI command strings

Symantec Endpoint Protection installation software uses Windows Installer (MSI) 3.1 or later packages for installation and deployment. If you use the command line to deploy a package, you can customize the installation. You can use the standard Windows Installer parameters and the Symantec-specific features and properties.

To use the Windows Installer, elevated privileges are required. If you try the installation without elevated privileges, the installation may fail without notice.

For the most up-to-date list of Symantec installation commands and parameters, see the article: [MSI command line reference for Symantec Endpoint Protection](#).

### NOTE

The Windows Installer advertise function is unsupported. Setaid.ini-specified features and properties take precedence over MSI-specified features and properties. Feature and property names in MSI commands are case-sensitive.

[About configuring Setaid.ini](#)

## About configuring Setaid.ini

Setaid.ini appears in all installation packages and controls many of the aspects of the installation, such as which features are installed. Setaid.ini always takes precedence over any setting that may appear in an MSI command string that is used to start the installation. Setaid.ini appears in the same directory as setup.exe. If you export to a single .exe file, you cannot configure Setaid.ini. However, the file is automatically configured when you export Symantec Endpoint Protection client installation files from the console.

The following lines show some of the options that you can configure in Setaid.ini.

```
[CUSTOM_SMC_CONFIG]
InstallationLogDir=
```

---

```
DestinationDirectory=  
[FEATURE_SELECTION]  
Core=1
```

```
SAVMain=1  
Download=1  
OutlookSnapin=1  
Pop3Smtplib=0  
NotesSnapin=0
```

```
PTPMain=1  
DCMain=1  
TruScan=1
```

## NOTE

The features are indented to show hierarchy. The features are not indented inside the Setaid.ini file. Feature names in Setaid.ini are case-sensitive.

Feature values that are set to 1 install the features. Feature values that are set to 0 do not install the features. You must specify and install the parent features to successfully install the client features.

### Be aware of the following additional setaid.ini settings that map to MSI properties for Symantec Endpoint Protection client installation:

- DestinationDirectory maps to PRODUCTINSTALLDIR
- KeepPreviousSetting maps to MIGRATESETTINGS
- AddProgramIntoStartMenu maps to ADDSTARTMENUICON

[Symantec Endpoint Protection command-line client features](#)

[Symantec Endpoint Protection command-line client installation properties](#)

[Windows Installer parameters](#)

## Symantec Endpoint Protection command-line client installation properties

These installation properties are for use with MSI command line installations.

**Table 211: Symantec Endpoint Protection client installation properties**

Property	Description
RUNLIVEUPDATE=val	<p><b>Determines whether LiveUpdate is run as part of the installation, where val is one of the following values:</b></p> <ul style="list-style-type: none"> <li>• 1: Runs LiveUpdate during installation (default).</li> <li>• 0: Does not run LiveUpdate during installation.</li> </ul> <p>By default, all Symantec Endpoint Protection clients in a group receive the latest versions of all content and all product updates. If the clients are configured to get updates from a management server, the clients receive only the updates that the server downloads. If the LiveUpdate Content policy allows all updates, but the management server does not download all updates, the clients receive only what the server downloads.</p>
ENABLEAUTOPROTECT=val	<p><b>Determines whether File System Auto-Protect is enabled after the installation is complete, where val is one of the following values:</b></p> <ul style="list-style-type: none"> <li>• 1: Enables Auto-Protect after installation (default).</li> <li>• 0: Disables Auto-Protect after installation.</li> </ul>
CACHE_INSTALLER=val	<p><b>Determines whether the installation files cache on the client, where val is one of the following values:</b></p> <ul style="list-style-type: none"> <li>• 1: Caches the installation files (default).</li> <li>• 0: Does not cache the installation files.</li> </ul>
MIGRATESETTINGS=val	<p><b>Determines the status of preserved settings in an upgrade scenario, where val is one of the following values:</b></p> <ul style="list-style-type: none"> <li>• 0: Does not preserve the settings or logs.</li> <li>• 1: Preserves all settings and logs.</li> <li>• 2: Preserves Sylink.xml and logs only.</li> </ul>
ADDSTARTMENUICON=val	<p><b>Determines whether or not to add the program to the Start Menu folder, where val is one of the following values:</b></p> <ul style="list-style-type: none"> <li>• 0: Does not add the program to the Start Menu folder.</li> <li>• 1: Adds the program to the Start Menu folder (default).</li> </ul>

## Installing Symantec Endpoint Protection client features using the command line

You can install the protection features by specifying them in Setaid.ini files and in MSI commands. Most features have a parent-child relationship. If you want to install a child feature that has a parent feature, you must also install the parent feature. For example, if you specify to install the Firewall feature but do not specify to install NTPMain, the firewall is not installed.

**Table 212: Symantec Endpoint Protection client features**

Feature	Description	Required parent features
Core	Installs the files that are used for communications between clients and Symantec Endpoint Protection Manager. This feature is required.	None
ADDefense	Installs the Endpoint Threat Defense for Active Directory component.	Core
DCMain	Installs the Application Control and Device Control feature.	PTPMain

Feature	Description	Required parent features
Download	Installs the complete protection for downloaded files. Includes fully functional reputation scanning by Download Insight.	SAVMain
Firewall	Installs the firewall feature.	NTPMain
ITPMain	Installs the Network and Intrusion Prevention and Browser Intrusion Prevention feature.	NTPMain
LANG1033	Installs English resources.	Core
NotesSnapin	Installs the Lotus Notes Auto-Protect email feature. Applies only to versions earlier than 14.2 RU1.	SAVMain
NTPMain	Installs the Network and Host Exploit Mitigation components.	Core
NTR	Installs the Network Traffic Redirection component.	Core
OutlookSnapin	Installs the Microsoft Exchange Auto-Protect email feature.	SAVMain
Pop3SmtP	Installs the protection for POP3 and SMTP mail. Available only on 32-bit systems. Applies only to versions earlier than 14.2 RU1.	SAVMain
PTPMain	Installs the Proactive Threat Protection components.	Core
SAVMain	Installs the virus, spyware, and basic download protection. Subfeatures install additional protection.	Core
TruScan	Installs the Behavioral Analysis (SONAR) feature.	PTPMain

## Windows Installer parameters

Symantec Endpoint Protection client installation packages use the standard Windows Installer parameters, as well as a set of extensions for command-line installation and deployment.

See the Windows Installer documentation for further information about the usage of standard Windows Installer parameters. You can also execute `msiexec.exe` from a command line to see the complete list of parameters.

**Table 213: Windows Installer parameters**

Parameter	Description
Sep.msi (32-bit) Sep64.msi (64-bit)	The installation file for the Symantec Endpoint Protection client. If the file name contains spaces, enclose the file name in quotations when used with <code>/I</code> and <code>/x</code> . Required
Msiexec	Windows Installer executable. Required
<code>/I ".msi file name"</code>	Install the specified file. If the file name contains spaces, enclose the file name in quotations. If the file is not in the same directory from which you execute <code>Msiexec</code> , specify the path name. If the path name contains spaces, enclose the path name in quotations. For example, <code>msiexec.exe /I "C:\path to\Sep.msi"</code> Required
<code>/qn</code>	Install silently.  <b>Note:</b> When a silent deployment is used, the applications that plug into Symantec Endpoint Protection, such as Microsoft Outlook, must be restarted after installation.
<code>/x ".msi file name"</code>	Uninstall the specified components. Optional

Parameter	Description
/qb	Install with a basic user interface that shows the installation progress. Optional
/!v logfilename	Create a verbose log file, where logfilename is the name of the log file you want to create. Optional
PRODUCTINSTALLDIR=path	Designate a custom path on the target computer where path is the specified target directory. If the path includes spaces, enclose the path in quotation marks.  <b>Note:</b> The default directory for 32-bit computers is C:\Program Files\Symantec\Symantec Endpoint Protection. The default directory for 64-bit computers is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection.  Optional
SYMREBOOT=value	Controls a computer restart after installation, where value is a valid argument. <b>The valid arguments include the following:</b> <ul style="list-style-type: none"> <li>• Force: Requires that the computer is restarted. Required for uninstallation.</li> <li>• Suppress: Prevents most restarts.</li> <li>• ReallySuppress: Prevents all restarts as part of the installation process, even a silent installation.</li> </ul> Optional  <b>Note:</b> Use ReallySuppress to suppress a restart when you perform a silent uninstallation of Symantec Endpoint Protection client.
ADDLOCAL= feature	Select the custom features to be installed, where feature is a specified component or list of components. If this property is not used, all applicable features are installed by default, and Auto-Protect email clients are installed only for detected email programs. To add all appropriate features for the client installations, use the ALL command as in ADDLOCAL=ALL. <a href="#">Symantec Endpoint Protection command-line client features</a>  <b>Note:</b> When you specify a new feature to install, you must include the names of the features that are already installed that you want to keep. If you do not specify the features that you want to keep, Windows Installer removes them. By specifying existing features, you do not overwrite the installed features. To uninstall an existing feature, use the REMOVE command.  Optional
REMOVE=feature	<b>Uninstall the previously installed program or a specific feature from the installed program, where feature is one of the following:</b> <ul style="list-style-type: none"> <li>• Feature: Uninstalls the feature or list of features from the target computer.</li> <li>• ALL: Uninstalls the program and all of the installed features. All is the default if a feature is not specified.</li> </ul> Optional

## Windows Security Center properties

You can customize Windows Security Center (WSC) properties during Symantec Endpoint Protection client installation. These properties apply to unmanaged clients only. Symantec Endpoint Protection Manager controls these properties for the managed clients.

### NOTE

These properties apply to Windows XP Service Pack 3 only. They do not apply to clients that run Windows Vista, or Windows 7 or later, except for the WSCAVUPTODATE property.

Windows Security Center was renamed to Action Center in Windows 7/8 and Security and Maintenance in Windows 10.



**Table 214: Windows Security Center properties**

Property	Description
WSCCONTROL=val	<b>Controls WSC where val is one of the following values:</b> <ul style="list-style-type: none"> <li>0: Do not control (default).</li> <li>1: Disable one time, the first time it is detected.</li> <li>2: Disable always.</li> <li>3: Restore if disabled.</li> </ul>
WSCAVALERT=val	<b>Configures the antivirus alerts for WSC where val is one of the following values:</b> <ul style="list-style-type: none"> <li>0: Enable.</li> <li>1: Disable (default).</li> <li>2: Do not control.</li> </ul>
WSCFWALERT=val	<b>Configures the firewall alerts for WSC where val is one of the following values:</b> <ul style="list-style-type: none"> <li>0: Enable.</li> <li>1: Disable (default).</li> <li>2: Do not control.</li> </ul>
WSCAVUPTODATE=val	Configures the WSC out-of-date time for antivirus definitions where val is one of the following values: 1 - 90: Number of days (default is 30).
DISABLEDEFENDER=val	<b>Determines whether to disable Windows Defender during installation, where val is one of the following values:</b> <ul style="list-style-type: none"> <li>1: Disables Windows Defender (default).</li> <li>0: Does not disable Windows Defender.</li> </ul>

## Command-line examples for installing the Windows client

**Table 215: Command-line examples**

Task	Command line
Silently install all of the Symantec Endpoint Protection client components with default settings to the directory C:\SFN. Suppress a computer restart, and create a verbose log file.	msiexec /I SEP.msi PRODUCTINSTALLDIR=C:\SFN SYMREBOOT=ReallySuppress /qn /l*v c:\temp\msi.log
Silently install the Symantec Endpoint Protection client with Virus and Spyware Protection, and with intrusion prevention and firewall. Force a computer restart, and create a verbose log file.	msiexec /I SEP.msi ADDLOCAL=Core,SAVMain,OutlookSnapin, Pop3SmtP,ITPMain,Firewall SYMREBOOT=Force /qn / l*v c:\temp\msi.log

## Installing Windows clients with Microsoft SCCM/SMS

You can use Microsoft System Center Configuration Manager (SCCM) to install Symantec client software. We assume that system administrators who use SCCM have previously installed software with SCCM. As a result, we assume that you do not need detailed information about installing Symantec client software with SCCM.

### NOTE

This topic also applies to Microsoft Systems Management Server (SMS).

### NOTE

This note applies to SMS version 2.0 and earlier: If you use SMS, turn off the **Show Status Icon On The Toolbar For All System Activity** feature on the clients in the **Advertised Programs Monitor**. In some

---

situations, Setup.exe might need to update a shared file that is in use by the Advertised Programs Monitor. If the file is in use, the installation fails.

Symantec recommends that SCCM/SMS packages launch Setup.exe rather than the MSI directly. This method enables installer logging. Use the custom package creation feature in SCCM/SMS to create custom packages instead of the package wizard feature.

#### **WARNING**

You should use a managed client installation package that you exported from Symantec Endpoint Protection Manager. If you use the client installation packages from the product download or the installation file, you deploy unmanaged clients. Unmanaged clients install with default settings and do not communicate with a management server.

[Installing Symantec Endpoint Protection clients with Save Package](#)

**Table 216: Process for installing the client using Microsoft System Center Configuration Manager / Systems Management Server**

Step	Description
Step 1	Export a managed client installation package from Symantec Endpoint Protection Manager that contains the software and policies to install on your client computers. By default, a managed client installation package contains a file named Sylink.xml, which identifies the server that manages the clients.
Step 2	Create a source directory and copy the Symantec client installation package into that source directory. For example, you would create a source directory and copy the Setup.exe file that you exported from Symantec Endpoint Protection Manager.
Step 3	In SCCM/SMS, create a custom package, name the package, and identify the source directory as part of the package.
Step 4	Configure the <b>Program</b> dialog box for the package to specify the executable that starts the installation process, and possibly specify the MSI with parameters.
Step 5	Distribute the software to specific <b>Collections</b> with <b>Advertising</b> .

For more information on using SCCM/SMS, see the Microsoft documentation that is appropriate for your version.

## **Installing Windows clients with an Active Directory Group Policy Object (GPO)**

You can install the Windows client by using a Windows Active Directory Group Policy Object. The procedures assume that you have installed this software and use Windows Active Directory to install client software with an Active Directory Group Policy Object.

The Symantec client installation uses standard Windows Installer (MSI) files. As a result, you can customize the client installation with MSI properties.

#### [About configuring MSI command strings](#)

You should confirm that your DNS server is set up correctly before deployment. The correct setup is required because Active Directory relies on your DNS server for computer communication. To test the setup, you can ping the Windows Active Directory computer, and then ping in the opposite direction. Use the fully qualified domain name. The use of the computer name alone does not call for a new DNS lookup. Use the following format:

ping computername.fullyqualifieddomainname.com

#### **WARNING**

You should use a managed client installation package that you exported from Symantec Endpoint Protection Manager. If you use the client installation packages from the product download or the installation file, you deploy

---

unmanaged clients. Unmanaged clients install with default settings and do not communicate with a management server.

#### [Installing Symantec Endpoint Protection clients with Save Package](#)

**Table 217: Steps for installing the client software by using Active Directory Group Policy Object**

Step	Action
Step 1	Export the managed client installation package with the option <b>Separate files (required for .MSI)</b> . <a href="#">Installing Symantec Endpoint Protection clients with Save Package</a>
Step 2	Stage the folder of installation files. For example, copy the managed client installation package into a shared folder on which you have set the correct permissions to allow access.
Step 3	Create a GPO software distribution. You should also test GPO installation with a small number of computers before the production deployment. If you do not configure DNS properly, GPO installations can take an hour or more. <a href="#">Creating a GPO software distribution</a>
Step 4	Add computers to the organizational unit. <a href="#">Adding computers to an organizational unit to install software</a>

#### [Uninstalling client software with an Active Directory Group Policy Object](#)

### Creating a GPO software distribution

If you use Microsoft Active Directory in your environment, you can use a GPO to deploy the Symantec Endpoint Protection client package to Windows computers. You create a software distribution then configure a GPO administrative template for the software packages.

This process assumes that you have installed Microsoft's Group Policy Management Console with Service Pack 1 or later. The Windows interface may be slightly different depending on the version of Windows you use.

This process also assumes that you have computers in the Computers group or some other group to which you want to install client software. Optionally, you can drag these computers into a new group that you create.

#### [Installing Windows clients with an Active Directory Group Policy Object \(GPO\)](#)

1. To create a GPO software distribution, on the Windows Taskbar, click **Start > All Programs > Administrative Tools > Group Policy Management**.
2. In the **Active Directory Users and Computers** window, in the console tree, right-click the domain, and then click **Active Directory Users and Computers**.

3. In the **Active Directory Users and Computers** window, select a target organizational unit (OU) under the appropriate domain.

You can also create a new OU for testing or other purposes. See Active Directory documentation by Microsoft for more information on how to create a new OU.

4. In the **Group Policy Management** window, in the console tree, right-click the organizational unit that you chose or created, and then click **Create and Link a GPO Here**.

You may need to refresh the domain to see a new OU.

- 
5. In the **New GPO** dialog box, in the Name box, type a name for your GPO, and then click **OK**.
  6. In the right pane, right-click the GPO that you created, and then click **Edit**.
  7. In the **Group Policy Object Editor** window, in the left pane, under **Computer Configuration**, expand **Software Settings**.
  8. Right-click **Software installation**, and then click **New > Package**.
  9. In the **Open** dialog box, type the Universal Naming Convention (UNC) path that points to and contains the MSI package.

Use the format as shown in the following example:

```
\\server name\SharedDir\Sep.msi
```

10. Click **Open**.
11. In the **Deploy Software** dialog box, click **Assigned**, and then click **OK**.

The package appears in the right pane of the Group Policy Object Editor window if you select Software Installation.

12. To configure administrative templates for the software package, in the **Group Policy Object Editor** window, in the console tree, display and enable the following settings:
  - **Computer Configuration > Administrative Templates > System > Logon > Always wait for the network at computer startup and logon**
  - **Computer Configuration > Administrative Templates > System > Group Policy > Software Installation policy processing**
  - **User Configuration > Administrative Templates > Windows Components > Windows Installer > Always install with elevated privileges**

**NOTE**

If you enabled User Account Control (UAC) on the client computers, you must also enable **Computer Configuration > Administrative Templates > Windows Components > Windows Installer > Always install with elevated privileges** to install Symantec client software with a GPO. You set these options to allow all Windows users to install Symantec client software.

13. Close the Group Policy Object Editor window.
14. In the **Group Policy Management** window, in the left pane, right-click the GPO that you edited, and then click **Enforced**.
15. In the right pane, under **Security Filtering**, click **Add**.
16. In the dialog box, under **Enter the object name to select**, type `Domain Computers`, and then click **OK**.

## **Adding computers to an organizational unit to install software**

You can add computers to an organizational unit to which Symantec Endpoint Protection installs by GPO. When the computers restart, the client software installation process begins. When users log on to the computers, the client software installation process completes. The group policy update, however, is not instantaneous, so it may take time for this policy to propagate. The following process contains the commands that you can run on the client computers to update the policy on demand.

---

## Installing Windows clients with an Active Directory Group Policy Object (GPO)

1. To add computers to the organizational unit to install software, on the Windows Taskbar, click **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.
2. In the **Active Directory Users and Computers** window, in the console tree, locate one or more computers to add to the organizational unit that you chose for GPO installation.

Computers first appear in the **Computers** organizational unit.

3. Drag and drop the computers into the organization unit that you chose or created for the installation.
4. Close the **Active Directory Users and Computers** window.
5. To update the GPO on demand on the client computers, open a command prompt on the client computers.
6. Type `gpupdate`, and then press **Enter**.

When complete, the command prompt window displays a message to let you know the policy update completed successfully. If an error message displays, follow the on-screen instructions for more information.

7. Close the command prompt window.

## Copying a Sylink.xml file to make a managed installation package

When you install Symantec Endpoint Protection Manager, it creates a file named `Sylink.xml` for each client group. Symantec Endpoint Protection clients read the contents of this file to know which management server manages the client. If you install the client from the installation file you get from Symantec, you install unmanaged clients. However, you can copy the `Sylink.xml` file to this folder before installation to install managed clients.

### NOTE

Packages that are exported with the Symantec Endpoint Protection Manager console are managed and already include a `Sylink.xml` file. To export a new managed package that you can deploy with a Group Policy Object, use the Client Deployment Wizard. Click **Save Package**, and check **Separate Files (required for .MSI)** when prompted.

### Installing Symantec Endpoint Protection clients with Save Package

To copy a `Sylink.xml` file to the product installation files to make a managed installation package

1. From Symantec Endpoint Protection Manager, export the `Sylink.xml` file from the correct client group and copy it to your computer.

### NOTE

You should create at least one new group with the management console before you export the `Sylink.xml` file. If you do not, the clients appear in the Default group.

### Adding a group

### Exporting the client-server communications file (Sylink.xml) manually

2. Copy the installation folder from the installation file you download to a folder on your computer. The folder `SEP` contains the 32-bit client, and the folder `SEPx64` contains the 64-bit client.

You can also use the installation folder for an unmanaged client package that you previously exported as separate files.

- 
3. Copy Sylink.xml to the installation folder. Replace the existing Sylink.xml file when prompted.

## Uninstalling client software with an Active Directory Group Policy Object

You can uninstall the client software that you installed with Active Directory.

### Uninstalling the Symantec Endpoint Protection client for Windows

To uninstall client software with an Active Directory Group Policy Object

1. On the Windows Taskbar, click **Start > All Programs > Administrative Tools > Group Policy Management**.  
The version of Windows that you use may display **Programs** instead of **All Programs** in the **Start** menu.
2. In the **Group Policy Management** window, in the console tree, expand the domain, expand **Computer Configuration**, expand **Software Settings**, right-click **Software Installation**, and then click **Properties**.
3. On the **Advanced** tab, check **Uninstall this application when it falls out of the scope of management**, and then click **OK**.
4. In the right pane, right-click the software package, and then click **Remove**.
5. In the **Remove Software** dialog box, check **Immediately uninstall the software from users and computers**, and then click **OK**.
6. Close the **Group Policy Object Editor** window, and then close the **Group Policy Management** window.

The software uninstalls when the client computers are restarted.

## Quick Start Guide for Symantec™ Endpoint Protection for Amazon Web Services

### Usage instructions and best practices for Symantec Endpoint Protection Manager on Amazon Web Services (AWS)

When you log on to Symantec Endpoint Protection Manager Amazon Machine Image (AMI) on Amazon Web Services for the first time, you should be aware of the following issues:

Item	Description
Initial logon credentials	When you connect to the instance for the first time, Symantec Endpoint Protection Manager opens automatically and then prompts you to change the password.
LiveUpdate launches after initial logon	When Symantec Endpoint Protection Manager LiveUpdate launches for the first time, it downloads more content than during subsequent LiveUpdate sessions. As a result, the responsiveness of the instance slows down until LiveUpdate completes. This behavior is expected, and only occurs on this initial launch. LiveUpdate launches five minutes after your initial logon to Symantec Endpoint Protection Manager.
Client does not appear immediately in Symantec Endpoint Protection Manager	You may notice that the client that is preinstalled on the instance does not immediately display on the <b>Home</b> tab in Symantec Endpoint Protection Manager. This behavior is expected. After the heartbeat into Symantec Endpoint Protection Manager completes, the client appears on the <b>Home</b> tab.
Update the email address for admin	You must change the default email address for <b>admin</b> in Symantec Endpoint Protection Manager. By default, the email address is a@b.com. You can easily change this email address after you log on to Symantec Endpoint Protection Manager in the <b>Admin</b> pane, under <b>Administrators &gt; Edit the administrator</b> . Since password recovery for Symantec Endpoint Protection Manager requires a valid email address, you should perform this task the first time you log on.

Item	Description
Update the database password	In version 14 or later, you can change the database password for Symantec Endpoint Protection Manager. You should change this password the first time you log on. <a href="#">Changing the password for an administrator account or the embedded database</a>
Remote push deployment (optional)	Symantec Endpoint Protection Manager push deployment makes use of the ICMP ping protocol to look up the IP address of an instance on the network. You must explicitly add the <b>ICMP Echo Request</b> ingress rule on client instance candidates in order for them to be visible on the Symantec Endpoint Protection Manager Client Deployment Wizard. To successfully deploy the client package from Symantec Endpoint Protection Manager to the client instances, you must enable TCP port 445 on the client instances. See the section Security Groups for more information.
Security Groups	The following tables demonstrate recommended security group firewall rules for AMI instances running Symantec Endpoint Protection: <ul style="list-style-type: none"> <li><a href="#">Incoming security group settings for Symantec Endpoint Protection instances</a></li> <li><a href="#">Outgoing security group settings for Symantec Endpoint Protection instances</a></li> </ul> For information on how to work with client instances, see: <a href="#">Amazon EC2 Security Groups for Windows Instances</a>

**Table 218: Incoming security group settings for Symantec Endpoint Protection instances**

Type / Protocol	Applies to	Port number	Source	Purpose
Custom TCP Rule / TCP	Symantec Endpoint Protection Manager	8014 443*	0.0.0.0/0	Used for HTTP communication between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection clients. * = Used for the optional HTTPS configuration.
Custom TCP Rule / TCP	Symantec Endpoint Protection Manager	8443	0.0.0.0/0	Used for HTTPS communication between a remote management console and Symantec Endpoint Protection Manager. All logon information and administrative communication takes place using this secure port.
Custom TCP Rule / TCP	Symantec Endpoint Protection Manager	8444	0.0.0.0/0	Used by the Symantec Endpoint Protection Manager web services.
Custom TCP Rule / TCP	Symantec Endpoint Protection Manager	8445	0.0.0.0/0	Used for HTTPS communication for the reporting console.
Custom TCP Rule / TCP	Symantec Endpoint Protection Manager	8765	0.0.0.0/0	Used for Tomcat shutdown.
Custom TCP Rule / TCP	Symantec Endpoint Protection Manager	9090	0.0.0.0/0	Used for the initial logon communication between a remote management console and Symantec Endpoint Protection Manager to display the logon screen.
Custom TCP Rule / TCP	Symantec Endpoint Protection client	445	0.0.0.0/0	Used for remote deployment of installation packages from Symantec Endpoint Protection Manager.
Custom ICMP Rule / Echo request	Symantec Endpoint Protection client	N/A	0.0.0.0/0	Used by Remote Push to look up the IP address of an Symantec Endpoint Protection client instance on the network.



Type / Protocol	Applies to	Port number	Source	Purpose
RDP / TCP	Symantec Endpoint Protection Manager, Symantec Endpoint Protection client	3389	0.0.0.0/0	Used to remotely connect to the instance.

**Table 219: Outgoing security group settings for Symantec Endpoint Protection instances**

Type / Protocol	Applies to	Port number	Destination
All traffic / All	Symantec Endpoint Protection Manager Symantec Endpoint Protection client	All	0.0.0.0/0

### Requirements to use Symantec Endpoint Protection Manager on Amazon Web Services

Amazon Web Services (AWS) account holders can subscribe to Symantec Endpoint Protection Manager on an Amazon Machine Image (AMI) on Amazon's Elastic Compute Cloud (EC2).

**Table 220: Prerequisites, supported platforms, and instances to run the Symantec Endpoint Protection Manager AMI**

Requirement	Details
Prerequisites	<p>The prerequisites to use Symantec Endpoint Protection Manager AMI for Amazon EC2 are as follows:</p> <ul style="list-style-type: none"> <li>You must have an AWS Marketplace account. To create an account or to access an existing account, go to: <a href="https://aws.amazon.com/marketplace">https://aws.amazon.com/marketplace</a></li> <li>If you use the Bring Your Own License (BYOL) option, you must have a valid license for Symantec Endpoint Protection. To review your licensing status, log on to the Broadcom Support Portal and go to the <a href="#">Broadcom Download Center</a>. Alternately, you can contact <a href="#">Symantec customer support</a> for non-technical questions about your license.</li> </ul>
Supported Platforms and Instances	<p>Symantec Endpoint Protection Manager AMI for Amazon EC2 (BYOL and Paid) includes support for:</p> <ul style="list-style-type: none"> <li>Symantec Endpoint Protection Manager, version 14 MP1 or later</li> <li>Windows Server 2012 R2 or later</li> </ul> <p>Symantec Endpoint Protection Manager AMI supports the following Amazon EC2 instances of Windows Server 2012 on the AWS Marketplace:</p> <ul style="list-style-type: none"> <li>10 client tier: m4.large (2x CPU, 8 GB RAM, EBS disk)</li> <li>100 client tier: m4.xlarge (4x CPU, 16 GB RAM, EBS disk)</li> <li>250 client tier: m4.2xlarge (8x CPU, 32 GB RAM, EBS disk)</li> <li>500 client tier: c4.2xlarge (8x CPU, 15 GB RAM, EBS disk)</li> </ul>

### Additional reference

For information on using Amazon EC2 and Symantec Endpoint Protection AMI, see: [Getting Started with AWS](#)

## What's new for Symantec Endpoint Protection (SEP) 14.0.1 (14 RU1)

### Protection features

- Cloud-based management using the Symantec Endpoint Protection cloud portal:** Symantec Endpoint Protection 14.1 includes a cloud portal that provides cloud-based management that extends Symantec Endpoint Protection's abilities to detect and remediate emerging threats in your environment. The cloud portal increases the visibility you



---

have into your network security posture with the dashboard views that provide insight into suspicious files across your devices. Symantec Endpoint Protection Manager seamlessly connects to the cloud through an internal bridge. You can also access the interface to the cloud portal directly.

You access the cloud portal Help for these features in the cloud portal.

- **Discover and block suspicious detections with an Intensive Protection policy:** The Intensive Protection policy settings tune multiple engines to improve detections. You can choose to log detections at a higher intensity so that you can see what files would be detected and blocked at that level. What-if logging helps you proactively whitelist any false positives before you decide to block the detections. When you apply this policy, some settings in Symantec Endpoint Protection Manager are ignored. For example, the Intensive Protection policy ignores the Bloodhound setting in the Virus and Spyware Protection policy.
- **Stronger support for low-bandwidth environments:** The cloud portal controls whether or not Symantec Endpoint Protection 14.0.1 clients receive updates less frequently for the clients that are on slower networks. In low-bandwidth mode, you can use the Intensive Protection policy to tune the security on your endpoints even more. These updates include virus, SONAR, and IPS definitions. The low-bandwidth improvements also include an automatic reduction of telemetry submissions data. Low bandwidth is off by default.
- **Integrated false positive management:** You can allow (whitelist) or block (blacklist) files from multiple views.
- **Additional Memory Exploit Mitigation features:** Memory Exploit Mitigation hardens the operating system to stop the attack on zero day regardless of the flaw, bug, or vulnerability in the software. Instead of waiting for a patch from the vendor and then scheduling time to apply the patch, Memory Exploit Mitigation handles the exploits immediately. Version 14.0.1 includes the following changes:
  - Generic Exploit Mitigation is renamed to Memory Exploit Mitigation.
  - The Memory Exploit Mitigation is a separate policy from the Intrusion Prevention policy.
  - Memory Exploit Mitigation includes more fine-tuned control to let you test and troubleshoot to mitigate false positives.
  - Memory Exploit Mitigation several new mitigation techniques
  - The command to remotely enable or disable Memory Exploit Mitigation on the Windows client changed from `smc -enable -gem` and `smc -disable -gem` to `smc -enable -mem` and `smc -disable -mem`.
- **Exceptions policy can exclude detections based on a file's certificate (Windows):** You can add exceptions for individual certificates to prevent the Windows client from scanning and detecting the signed files as suspicious. For example, a tool that your company developed internally may use a self-signed certificate. Excluding this certificate from scans prevents Auto-Protect, Download Insight, SONAR, or other scans from detecting the files that it signs as suspicious.
- **Updated EDR integration with Symantec Advanced Threat Protection:** Endpoint Symantec Advanced Threat Protection: Endpoint (ATP) is an on-premises virtual appliance that detects advanced threats on endpoints in your network. ATP: Endpoint delivers actionable data so that you can quickly analyze and respond to the threats. The ATP module provides Endpoint Detection and Response (EDR), which allows for direct communication with registered client computers. EDR greatly improves the time for client computers to receive commands for evidence of compromise (EOC) searches and file remediation. A new version of the EDR component allows for collection of events on a client computer. EDR includes information on files, processes, registries, and network connections. This data is submitted to the ATP: Endpoint console. The newest version of EDR requires the ATP: Endpoint 3.0 product, and is not licensed in Symantec Endpoint Protection itself. You can download the latest EDR content through LiveUpdate.
- **Symantec Endpoint Protection Deception:** Deception is used to detect adversary activity at the endpoint using "deceptors." The underlying assumption with this approach is that the attacker has already breached the primary defenses of the network and performs reconnaissance in the environment. The attacker looks to find critical assets, like a domain controller or database credentials. With Deception, you can more quickly detect infiltration attempts. You can download a sample deceptor through FileConnect, either in the Tools directory on the full installation file or as a standalone download.
- **Advanced Machine Learning (AML) for Mac clients:** The AML engine now works with the Symantec real-time cloud-based threat intelligence on Mac clients. AML enables Symantec Endpoint Protection to detect malware in the pre-execution phase, thereby stopping large classes of malware, both known and unknown.

## Management server features

- The option to enable notifications on the Symantec Endpoint Protection Manager and the Windows client has changed from Display Intrusion Prevention notifications to Display Intrusion Prevention and Memory Exploit Mitigation notifications. In versions 12.1.6.x and earlier, this option works for IPS notifications only.
- In the Computer Status logs and quick reports, Network and Host Exploit Mitigation Protection off changed to Firewall off and Proactive Threat Protection off changed to SONAR off. To access the log, click **Monitors > Logs tab > Computer Status log type > Additional Settings > Compliance options**. To access the quick reports, click **Reports > Quick Reports tab > Computer Status report type > Additional Settings > Compliance options**.
- **Enable/Disable Network and Host Exploit Mitigation** mixed mode setting has been renamed to **Enable/Disable Network Threat Protection**. In 14 MPx versions, in the Client/Server Control Settings tab for mixed mode, the **Enable/Disable Network and Host Exploit Mitigation** command is not correctly named. This command is for the firewall and the intrusion prevention system only (Network Threat Protection), and not Memory Exploit Mitigation.

## System requirements

Symantec Endpoint Protection 14.0.1 adds support for:

- SQL Server 2016 SP1 for use with Symantec Endpoint Protection Manager
- macOS 10.13 (High Sierra)
- Windows 10 Fall Creators Update (2017) (32-bit, 64-bit)
- Browser support: Mozilla Firefox 5.x through 56.x, Google Chrome 61.0.x

## Client installation

- **The Client Deployment Wizard includes host name and IP address column labels:** To install new clients using remote push, you search for available computers in your network. Previously, the list of the available computers had appeared in a random order. Now, you can sort the computers by alphabetical or numerical order using new host name and IP address columns. You can then find the computers you want to install the clients on quicker. The labels appear in the Client Deployment Wizard. On the Computer Selection panel, click Search Network, and then click Find Computers.
- **Password required to uninstall the Mac client:** You can now require that the user enter a password to uninstall the Mac client.
- **Symantec Endpoint Protection kernel authorization required as of macOS 10.13:** macOS 10.13 adds a security requirement that kernel extensions be authorized. Symantec Endpoint Protection 14.0.1 adds support for macOS 10.13. If the kernel extension needs to be authorized, you are prompted during the installation of the Mac client. If you do not authorize the kernel extension, the Mac client cannot properly function. To authorize the kernel extension, click Allow in the Security & Privacy system preference. You do not need to provide administrator credentials. You only need to authorize the kernel extension once. If you uninstall and reinstall the client, or upgrade your operating system to 10.13 with version 14 installed, you do not need to reauthorize. Kernel authorization is required even when you use Remote Push. You must take this additional step after using Remote Push to deploy Symantec Endpoint Protection.
- **Option for Add Client Install Package renamed:** In version 14, the option for Include latest content in the client installation package was incorrectly changed to Include virus definitions in the client installation package. To more accurately describe this option, this option is changed to Include new content types in the client installation package.

## REST API commands

- The Symantec Endpoint Protection Manager REST APIs enable programmatic interaction with Symantec Endpoint Protection. This set of REST APIs connect to and perform Symantec Endpoint Protection Manager operations from Symantec Advanced Threat Protection: Endpoint (ATP) and Symantec Web Gateway (SWG). You use the APIs if you do not have access to Symantec Endpoint Protection Manager. Note: If Symantec Endpoint Protection Manager is enrolled with the cloud portal, using REST API commands to manage what that the cloud portal manages is not supported.
- The documentation is located on the Symantec Endpoint Protection Manager server at the following address, where SEPM-IP is the IP address of the Symantec Endpoint Protection Manager server: <https://SEPM-IP:8446/sepm/restapidocs.html>

## Removed or unsupported features

- 
- **End of Life announced for Endpoint Protection 12.1.x:** On April 3, 2017, Symantec announced the End of Life for Endpoint Protection 12.1.x. The End of Life date starts the process that leads to the end of support for all released versions of 12.1. These released versions include release updates and maintenance patches.
  - **Removed option to manually submit quarantined threats to Symantec Security Response:** In version 14 and earlier, you can submit threats in the quarantine manually from Windows clients to the Security Response team. As of version 14.0.1, you can submit these samples automatically only to a Central Quarantine Server.
  - In Symantec Endpoint Protection Manager, the **Allow client computers to manually submit quarantined items to Symantec Security Response** option was in the **Virus and Spyware Protection policy > Quarantine > General** tab.
  - On the Windows client, click **View Quarantine**. The **Submit** option and the right-click **Submit** menu item were removed.
  - Removed support for Mac OS X 10.9
  - **Host Integrity policy options for Mac:** Host Integrity policies for Mac required the installation of the Symantec Network Access Control On-Demand client for Mac. Symantec Network Access Control has reached End of Life, and is not supported for use with Symantec Endpoint Protection 14.x. While the Mac options are still in the user interface, they are not supported.

## What's new in Symantec Endpoint Protection (SEP) 14

### Protection features

- **Intelligent Threat Cloud Service for client installation packages (Windows):** Version 14 includes three new sizes of client installation packages, based on which set of virus definitions they include:
  - **Standard client:** Designed for typical installations where clients have access to the cloud or the clients are version 12.1.6 and earlier. The standard client is 80% to 90% smaller than a dark network client installation package and includes the most recent virus definitions only. After installation, the client accesses the full set of virus definitions from the cloud.
  - **Embedded client or VDI client:** The embedded client replaces the reduced-size client that was introduced in version 12.1.6. The embedded client is smaller than the standard client and also includes the most recent virus definitions only. After installation, the client accesses the full set of virus definitions from the cloud.
  - **Dark network client:** Installs a full set of virus definitions and keeps the definitions locally rather than accessing them from the cloud. Use this client installation package if the client computers are in networks with no access to the cloud.
- **Generic Exploit Mitigation (Windows):** prevents common vulnerability attacks in typical software applications. Generic Exploit Mitigation installs with intrusion prevention and includes the following types of protection: Java exploit prevention, heap spray mitigation, and structured exception handling overwrite protection (SEHOP). The protections apply to the specific applications that are listed in the Intrusion Prevention policy. Symantec Endpoint Protection downloads the application list as part of its LiveUpdate content. To see the list of applications, open an Intrusion Prevention policy and then click **Generic Exploit Mitigation**.
- **SONAR/Auto-Protect:**
  - **Enable Suspicious Behavior Detection** option (Windows): You can enable or disable suspicious behavior detection if SONAR is disabled. Therefore, you can have behavior policy enforcement protection of applications on while SONAR scoring is off.
  - **Scan files on remote computers** option (Windows, Linux): You can disable the option for SONAR or Auto-Protect to scan files on computers on other networks. Disabling this option increases performance. However, you should keep this option enabled as SONAR looks for worms such as Salinity, which infects network drives. For Auto-Protect scans all files reduces and reduces the client computer's performance, you can enable the **Only when files are**

---

**executed** option. To access these options, click **Policies > Virus and Spyware Protection policy > SONAR or Auto-Protect**.

- **Virus scan logic moved to Auto-Protect user mode:** Auto-Protect user mode reduces kernel memory usage and provides greater system health. In rare cases of crashes, the computer does not blue screen and is recoverable.
- **Emulator for packed malware:** For Auto-Protect and virus scans, a new emulator improves scan performance and effectiveness by at least 10 percent. This anti-evasion technique addresses packed malware obfuscation techniques and detects the malware that is hidden inside custom packers.
- **Advanced Machine Learning (AML) on the endpoint for improved static detections:** This new endpoint-based machine learning engine can detect malware based on static attributes. This technology enables Symantec Endpoint Protection to detect malware in the pre-execution phase, thereby stopping large classes of malware, both known and unknown. The AML engine works with the Symantec real-time cloud-based threat intelligence to provide best-in-class protection with low false positives.
- **Insight Lookup (Windows):**
  - You can still enable or disable Insight Lookup for version 14 and legacy 12.1.x clients, but you cannot set the sensitivity level or action settings. Instead, Insight Lookup uses internal settings to optimize the scan because Download Insight detections are now completely handled by real-time protection. The new **Enable Insight Lookup** option on the **Scan Details** tab replaces the **Insight Lookup** tab in version 12.1.x. Click the **Virus and Spyware Protection policy > Administrator-Defined Scans**, choose either scheduled scans or on-demand scans, and then click **Scan Details**.
  - On standard and embedded/VDI clients, Insight Lookup now allows Auto-Protect, scheduled scans, and manual scans to look up both file reputation information and definitions in the cloud. However, the dark network clients include the full set of definitions and do not use Insight Lookup. You enable Insight Lookup in the **Clients > Policies tab > External Communications > Submissions** tab.
- **Scheduled and on-demand scans support the %systemdrive% and %userprofile% variables (Windows):** These scans let you select specific folders to be scanned rather than scanning all the files on the Windows client computer. The %systemdrive% variable indicates the location where the Windows operating system is installed. The %userprofile% variable corresponds to the user profile folders for the users who are logged on. You can also exclude these folders from being scanned by using an Exceptions policy.
- **Reports display an application's hash value you can use to block applications:** You can use the hash value instead of an application's name to add to the policies that block applications. The hash value is unique whereas an application name may not be. To find the hash value, look in the **Hash Type / Application Hash** column in the following reports:
  - **Risk** reports: Infected and At Risk Computers; Download Risk Distributions; SONAR Detection Results; SONAR Threat Distribution; Symantec Endpoint Protection Daily Status Report; and Symantec Endpoint Protection Weekly Status Report. To view the Risk reports, click **Reports > Quick Reports > Risk**.
  - **Home page > Activity Summary** link
- **Client submissions and server data collection:** You can enable Symantec Endpoint Protection to send information about detected threats and your network configuration to Symantec. Symantec uses this information for additional analysis and to improve the security features in the product.
  - Version 14 has several new types of client submissions that you can enable. You access these options by clicking **Clients > Policies tab > External Communications > Submissions tab > More options**.
  - The previously existing submission types are automatically submitted with the **Send anonymous data to Symantec to receive enhanced threat protection intelligence** option. In 12.1.6.x and earlier, this option was labeled **Let computers automatically forward selected anonymous security information to Symantec**.
  - You use the new **Send client-identifiable data to Symantec for custom analysis** option if you participate in a Symantec-sponsored program to get recommendations specific to your security network.
  - For server data collection, the **Yes, I would like to help optimize Symantec's endpoint security solutions by submitting anonymous system and usage information to Symantec** option is now labeled **Send anonymous**

---

**data to Symantec to receive enhanced threat protection intelligence.** You access this option on the **Admin > Servers > Edit Site Properties > Data Collection** tab.

- **LiveUpdate downloads new types of content:** Symantec Endpoint Protection Manager downloads additional types of content from LiveUpdate servers:
  - Client security patches
  - Endpoint Detection and Response: Definitions that the Endpoint Detection and Response (EDR) component uses to detect and investigate suspicious activities and issues on hosts and endpoints.
  - Common Network Transport Library and Configuration: Definitions that the entire product uses to achieve network transportation and telemetry.

## System requirements

Operating system	<ul style="list-style-type: none"><li>• Symantec Endpoint Protection Manager:<ul style="list-style-type: none"><li>– Windows Server 2016</li></ul></li><li>• Linux client:<ul style="list-style-type: none"><li>– Red Hat Enterprise Linux (RHEL) 7.1 and 7.2 (precompiled binary support)</li><li>– Oracle Linux (OEL) 6U5</li></ul></li><li>• Mac client:<ul style="list-style-type: none"><li>– MacOS 10.12 (Sierra)</li></ul></li></ul>
Database	SQL Server 2014 SP2
Web browser	For the Symantec Endpoint Protection Manager web console and Help: <ul style="list-style-type: none"><li>• Microsoft Edge</li><li>• Mozilla Firefox 5.x through 49.0.1</li><li>• Google Chrome through 54.0.x</li></ul>
Other	<ul style="list-style-type: none"><li>• net-tools or iproute2 (Linux client communication)</li><li>• LiveUpdate on the Linux client no longer requires the installation of Java.</li></ul>

## Symantec Endpoint Protection Manager installation

The DVD installation screen is simpler with fewer screens:

- You can install Symantec Endpoint Protection Manager from the first screen rather than a later screen.
- You can link to the *Quick Start Guide*, which describes how to deploy 500 or fewer clients with the default installation.

## Management Server Installation Wizard

- The installation wizard now displays the available hard drive space for local drives, but not the hard disk space for USB thumb drives or disc drives. The wizard does not let you install the management server unless the computer meets the minimum system requirements. The installation proceeds if the computer meets the recommended system requirements. The recommended minimum hard drive space the management server needs on a system drive is 40 GB. On an alternative drive, the management server needs 15 GB (system drive) and 25 GB (installation drive).
- **Symantec Endpoint Protection Manager installs with the HTTPS protocol:** When you install Symantec Endpoint Protection Manager for the first time, it uses the HTTPS protocol by default to communicate between the management server and the clients. If you upgrade from an earlier version, Symantec Endpoint Protection Manager retains the protocol from the earlier version. For the upgrades that use HTTP, you can create a new management server list that uses HTTPS and switch to the list in the **Communications Settings** dialog box.

## Symantec Endpoint Protection Manager configuration

### Management Server Configuration Wizard

- 
- Changed the default installation from 100 clients or fewer to 500 clients or fewer.
  - Merged the administrator's email address and test email screens into one screen, and improved the workflow for testing the administrator's email address.
  - Includes an option to support TLS communication with the mail server, **Prepare the server to use a secure connection**. You also configure TLS communication in the **Server Properties** dialog box. In earlier versions, only SSL is available. In addition, you can test the mail server connection at any time instead of during installation only.
  - The **Run LiveUpdate** screen and partner information is merged into one screen.
  - Removed the default configuration settings confirmation page. These details are now written in the `SEPMConfigurationSettings.txt` file that is located in the `<SEPM installation folder>\tomcat\etc` folder. When you upgrade from previous releases, Symantec Endpoint Protection Manager creates this text file.
  - While you wait for the installation wizard to create the embedded database, a progress bar shows how far the installation has progressed.

**Reset the embedded database password:** If you forget or want to change the embedded database password, run the Management Server Configuration Wizard and reconfigure the management server. On the Windows Start menu, click **All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Tools > Management Server Configuration Wizard**.

### Symantec Endpoint Protection Manager console

- **New user interface:** Symantec Endpoint Protection Manager now has an updated cloud look and feel with new icons and fonts. For example:
  - The client status icons changed.
  - Inherited firewall rules are italicized instead of shaded purple.
- The name of the **Welcome** page changed to the **Getting Started** page.
- The **Getting Started** page displays a list of required tasks to perform before you install for the first time or upgrade:
  - **Run LiveUpdate now:** LiveUpdate has run on Symantec Endpoint Protection Manager and downloaded at least one set of valid virus definitions. Or, LiveUpdate has connected to a Symantec Endpoint Protection client and downloaded at least one set of valid virus definitions.
  - **Activate your product:** The license needs to be valid and cannot be either over-deployed, a trial version, upgrade, invalid, or expired.
  - **Install the client software on your computers:** At least one Symantec Endpoint Protection client needs to be connected to the management server. The **Home page > Security Status** pane also indicates whether or not a minimum of one client is installed. The **Getting Started** page reappears until all the required tasks are completed. Then a **Do not show this page again** check box appears at the bottom of the screen. You can redisplay the **Getting Started** page in the **Help** menu.

### Client installation

- The **Client Deployment Wizard** has the following upgrades to make it easier to install the clients:
  - The command to open the Client Deployment Wizard has changed from Add a client to Install a client. You access the wizard by clicking either the **Clients pane > Tasks**, or by clicking the **Help menu > Getting Started > Required tasks > Install the client software on your computers**.
  - The **Client Install Settings** dialog box has the following new options:



- **Remove existing Symantec Endpoint Protection client software that cannot be uninstalled** uninstalls an existing Symantec Endpoint Protection client when other installation methods do not work. Only use this feature to remove corrupted or malfunctioning installations of the Symantec Endpoint Protection client.
- **Do not uninstall existing security software** is the default setting, which you use if you do not need to uninstall any security software from the client computer.
- The wizard uninstalls more third-party security products. See Third-party security software removal in Endpoint Protection. You access these options either through the Client Deployment Wizard or through the **Admin > Install Packages > Client Install Settings** dialog box.
- In the **Select Group and Install Feature Sets** pane of the wizard, the **Include all content in the client installation package** option has changed to **Include virus definitions in the client installation package**. The meaning of the check box is clearer. This option is in the **Admin > Install Packages > Export a Client Install Package** dialog box. This option replaced the **Select** option.
- **Preferred mode options removed:** The preferred mode options have been removed because the wizard installs the clients in computer mode by default. You can change the mode to user mode, but Symantec recommends that you continue to use computer mode.

### Management server features

- **Custom replication schedule:** You can now run replication multiple times a day, which improves effective reporting while preventing deadlocks on Symantec Endpoint Protection Manager. Previously, the replication schedule only ran either once an hour or once a day, which was either too often or too infrequently. For some companies, security requirements and customer reporting requirements means that daily replication is not enough. For companies with large network environments, hourly replication between dedicated management servers might be too often and might not complete before the next replication period starts. See How to install a second site and configure it for replication.
- **Subnet mask for explicit Group Update Providers:** In the LiveUpdate Settings policy, you can now reduce the number of explicit Group Update Provider entries by adding a client subnet mask. The subnet mask lets you add a larger subnet which can encompass multiple subnets, reducing the number of explicit entries from thousands to a few. In previous releases, you had to manually add the IP address for each client to be sure that the explicit GUP entry was applied to that client. For example, rather than having to enter both the 192.168.1.0 and 192.168.2.0 subnet, you can add the 192.168.0.0 subnet and the 255.255.0.0 subnet mask. See Configuring clients to download content from Group Update Providers. See About the types of Group Update Providers.
- **In-product notifications:** You can read the latest news about Symantec Endpoint Protection by clicking the **Latest News** link on any main console page, which opens the **Endpoint Protection Notifications** webpage. A bell icon appears whenever there is new news or alerts on the webpage. After you open the webpage, the bell icon disappears. In previous versions you had to manually and repeatedly check the Symantec Endpoint Protection Support page for information.
- **TLS 1.2 communication:** The communication between management server to management server and management server to client migrated away from SSL and earlier versions of TLS to TLS 1.2.
- **Administrator accounts:** The overview page for an administrator account displays the following options: **Password Verification Attempt Threshold** displays the number of logon attempts administrators can make with an invalid password before Symantec Endpoint Protection Manager locks them out. **Failed Password Verification Attempts** displays the number of failed logon attempts an administrator made.
- The **Test Account** option on the **Authentication** tab has changed to **Check Account**. This option checks whether the administrator account name exists in the connected Active Directory server or the LDAP server.
- The **Advanced Settings** link has changed to **Additional Settings** on the **Monitors** page > **Logs** tab and **Reports** page > **Quick Reports** tab.

### Client features

- **Device control (Mac):** You can now configure a Device Control policy for Mac clients. Device control controls the use of removable devices, such as USBs and FireWire. The policy supports permissions for reading, writing, and executing, and supports devices based on the type, make, model, or serial number.
- **AutoUpgrade (Mac):** You can automatically update the Mac client from Symantec Endpoint Protection Manager.
- **Security patches for the client (Windows):** You can now download and install security fixes for Windows clients using LiveUpdate, a Group Update Provider, or the management server. This option lets customers receive security fixes as easily as they receive virus definition updates. To download the security fixes to a management server, make sure that the option is enabled for the site. To download the security fixes to the clients, use the **Download security patches to fix the vulnerabilities in the latest version of the Symantec Endpoint Protection client** option in a LiveUpdate Settings policy.
- **Troubleshooting client crashes (Windows):** If the client crashes or behaves abnormally, a new component collects information about the client and reports it to a Symantec server. Symantec can use this information to better understand the cause of the crash, and improve the product. To enable this option, click **Admin > Servers > Edit Site Properties > Data Collection** tab, and make sure that **Let clients send troubleshooting information to Symantec to resolve product issues faster** is checked.
- **Symantec Endpoint Protection client drivers for the Windows 10 Device Guard (Windows):** Windows 10 includes a new feature that is called Device Guard that lets you lock down devices against new and unknown malware variants as well as advanced persistent threats (APTs). Device Guard uses hardware technology and virtualization to isolate hypervisor-related functions from the rest of the Windows operating system.

## API references

- Symantec Endpoint Protection Manager includes a set of REST APIs that connect to and perform Symantec Endpoint Protection Manager operations from Symantec Advanced Threat Protection (ATP). You use the APIs if you do not have access to Symantec Endpoint Protection Manager. The documentation is located in the following places:
  - On the Symantec Endpoint Protection Manager server at the following address, where SEPM-IP is the IP address of the Symantec Endpoint Protection Manager server: <https://SEPM-IP:8446/sepm/restapidocs.html>
- The API for remote monitoring and management (RMM) includes a new command, `assignQuarantinePolicy`. This command assigns a policy to one or more of the group's Quarantine locations. In addition, the RMM API documentation folder was renamed from `Tools\Integration` to `Tools\WebServicesDocumentation`.
- The `semapisrv` service listens for API commands for the Symantec Endpoint Protection Manager.

## Tools

The tools in this list are located in the installation file that you download from FileConnect in the `\Tools` folder, unless otherwise noted.

- **DeviceInfo (Mac):** The DeviceInfo tool lets you obtain the device vendor, model, or serial number for a specific device on the Mac client to use in Device Control policies. The tool is located in the `\Tools\DeviceInfo` folder.
- **TLS to Microsoft SQL Server database support:** Symantec Endpoint Protection Manager communicates with the SQL Server over an encrypted channel by default. The `SetSQLServerTLSEncryption.bat` tool lets you disable or enable TLS encryption between the management server and the Microsoft SQL Server communication. As of version 14, it can be used with the management server installations that are configured to use the Microsoft SQL Server database. You access the tool from `<installation directory>\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools`.
- **SymDiag replaces SymHelp:** The SymHelp tool was renamed as the Symantec Diagnostic (SymDiag) tool. SymDiag is a multi-product diagnostic tool that identifies common issues, gathers data for support-assisted troubleshooting, and provides links to other customer self-help and support resources.
- **Content Distribution Monitor:** The Content Distribution Monitor tool monitors management servers, clients, and GUPs in your environment. The tool shows a graphical display of the health and content distribution status, site throughput, and database table records. A new Site Information tab displays the throughput data that is collected after the last heartbeat between this site's management servers and the client computers. The tool is located in the `\Tools`



---

\ContentDistributionMonitor folder. In previous versions, this tool was not supported. The tool was also called SEPMMonitor.

- **SEPPrep tool was removed:** The unsupported SEPPrep tool was used in previous releases to remove third-party competitor's security software and Symantec software remotely or by using a script. The Client Deployment Wizard includes options in the Client Install Settings dialog box to uninstall both third-party products and Symantec products. To uninstall Symantec Endpoint Protection remotely, you can also download the CleanWipe tool from the Tools\Cleanwipe folder.
- **The Quarantine Server and Quarantine Console folder was removed:** The Central Quarantine Server and Quarantine Console has been removed from the Symantec Endpoint Protection installation screen and the Tools\CentralQ folder. You can still use the Central Quarantine tool, but you can only download it from a previous version of Symantec Endpoint Protection.

## Removed or unsupported features

- Symantec Endpoint Protection Manager no longer supports:
  - An installation on Windows Server 2003, any desktop operating system, or any 32-bit operating system.
  - SQL Server 2005, SQL Server 2008 SP3 and earlier, and SQL Server 2008 R2 SP2 and earlier.
  - Migration from Symantec Endpoint Protection Manager 11.x or 12.0 to 14. You must first upgrade to the latest version of 12.1, or uninstall the older Symantec Endpoint Protection Manager. Symantec Endpoint Protection Manager displays a warning for 11.x or 12.0 to 14 migrations.
  - The ability to import a client installation package for 11.x.
- The Symantec Endpoint Protection Manager web console no longer supports Internet Explorer 8, 9, or 10.
- The Symantec Endpoint Protection client no longer supports:
  - An installation on any version of Windows XP / Server 2003.
  - An installation on any version of Windows Embedded that is based on Windows XP, such as Windows Embedded Standard 2009.
  - Mac OS X 10.8.
  - Updates for 11.x or 12.0 clients. Symantec Endpoint Protection 11.x clients can no longer get updated content from Symantec Endpoint Protection Manager. To continue to protect and get the best security possible for 11.x client computers, you should upgrade your clients from version 11.x to 14. You can also run a report that displays which computers still have Symantec Endpoint Protection Manager 11.x or 12.0 installed. Click the **Monitors > Notifications** tab to add a notification to display a list of computers with the unsupported 11.x and 12.0 versions installed.
- **Symantec Network Access Control** reaches end-of-life support between September and November 2017. Version 14 does not support Symantec Network Access Control. If you want to use Symantec Network Access Control, you should use version 12.1.5 or earlier. In addition, the Symantec Endpoint Protection Manager Help no longer includes the documentation on Symantec Network Access Control features.
- The vShield-enabled Shared Insight Cache (VSIC) and Security Virtual Appliance (SVA) are no longer supported. In the Virus and Spyware Protection policy, the **Windows Settings > Miscellaneous > Shared Insight Cache** tab no longer has the **Enable Shared Insight Cache** or **Shared Insight Cache using VMware vShield** options. Instead, you check or uncheck **Shared Insight Cache using Network**. Symantec Endpoint Protection still provides the Shared Insight Cache and Virtual Image Exception features for virtual infrastructures. You can also run Symantec Data Center Security: Server and Symantec Endpoint Protection together.
- The **Home page > Common tasks** menu was removed. The **Common tasks** menu was previously a list of the required tasks. To view the list of both common tasks and required tasks, click **Help > Getting Started page**. The Getting Started page also appears when you upgrade or when any one of the required tasks have not been completed.
- The **Require standard HTTP headers for LiveUpdate connection** option in the **LiveUpdate Settings policy > Advanced Settings** tab was removed. In 12.1.6, you enable this option to require standard HTTP headers for the LiveUpdate connection if the connection used nonstandard headers that your non-Symantec Endpoint Protection

---

firewall might block. By default, Windows, Mac, and Linux clients are required to use standard HTTP headers, so the option is no longer necessary.

- The options for limited administrators being able to run reports for the clients and the servers that run Symantec AntiVirus 10.x and earlier was removed. Symantec Endpoint Protection does not support or update the content for Symantec AntiVirus clients.
- The **Applies To** column for an **Exceptions policy > Windows Application Exception** was removed. The **Applies To** column was used for 11.0.x clients and 12.1.x and later clients. Because 11.0.x clients are no longer supported, this information is not needed.

## Documentation

- You can review a new *Quick Start Guide*, which describes how to get Symantec Endpoint Protection installed and running immediately. Use this method if you have fewer than 500 clients with a default installation.
- Version 14 does not include a *Getting Started Guide*. Instead, see the Getting Started chapter of the *Symantec Endpoint Protection Installation and Administration Guide* for a customizable installation. This chapter includes the same topics that used to be in the *Getting Started Guide*.

---

## Glossary

---

Review definitions of some terms

The glossary defines technologies that Symantec Endpoint Protection uses.

### Bloodhound

Bloodhound isolates and locates the logical regions of a file to detect a high percentage of unknown viruses. Bloodhound then analyzes the program logic for virus-like behavior.

### Early Launch Anti-Malware

Early launch anti-malware (ELAM) protects client computers from threats that load at startup. Symantec Endpoint Protection includes an early launch anti-malware driver that works with the Microsoft early launch anti-malware driver to provide the protection. The settings are supported on Microsoft Windows 8 and Windows Server 2012.

The early launch anti-malware driver is a special type of driver that initializes first and inspects other startup drivers for malicious code. When the Symantec Endpoint Protection driver detects a startup driver, it determines whether the driver is good, bad, or unknown. The Symantec Endpoint Protection driver then passes the information to Windows to decide to allow or block the detected driver.

The Symantec Endpoint Protection settings provide an option to treat bad drivers and bad critical drivers as unknown. Bad critical drivers are the drivers that are identified as malware but are required for computer startup. By default, Windows allows unknown drivers to load. You might want to select the override option if you get any false positive detections that block an important driver. If you block an important driver, you might prevent client computers from starting up.

The Windows early launch anti-malware driver must be enabled for the Symantec Endpoint Protection settings to take effect. You use the Windows Group Policy editor to view and modify the Windows ELAM settings. See your Windows documentation for more information.

### File Reputation

The file reputation indicates how potentially harmful or not harmful a file might be. Symantec determines a file's reputation by collecting information about the file's characteristics.

### Insight

Insight allows scans to skip digitally signed files and trusted good files. Some files contain typical vulnerabilities. After those files are scanned initially, subsequent scans can skip the files since vulnerability definitions rarely change. Insight also uses file reputation data to skip trusted files. You can configure the level of trust. If you select **Symantec and Community Trusted**, scans skip more files (less secure). If you select **Symantec Trusted**, scans skip fewer files (more secure).

When scans skip files, the scan performance might improve.

### Insight Lookup

Insight Lookup provides some cloud protection for 12.1.x clients. Insight Lookup runs as part of scheduled or manual scans and checks the reputation of files that were downloaded from a supported portal. Insight Lookup gets the reputation information from the Symantec reputation database (Symantec Insight) in the cloud. Reputation data is the information about the potential maliciousness of a file, based on information from Symantec's global intelligence network.

---

Starting in 14, you cannot configure a sensitivity level for Insight Lookup. Insight Lookup uses the Download Insight sensitivity.

#### **NOTE**

Insight Lookup does not run on right-click scans of folders or drives. It does run on right-click scans of selected portal files.

## **What is an .slf file?**

Symantec license files use the file extension .slf (Symantec license file). When you purchase a license, you may receive a Symantec license file by email, or you can download it. Note that when the license file is sent in email, it is attached to the email as a .zip file. The .slf file is contained within the .zip file.

A license file contains one or more license keys that are required to activate one or more features of a Symantec product. License files contain secure XML data that is specific to each product. The license file cannot be altered without corrupting and invalidating the license.

You can import an .slf file to activate your Symantec product. You use the License Activation Wizard to import the file into Symantec Endpoint Protection Manager.

To purchase licenses, contact your [preferred reseller](#).

## **Risk Categories**

Symantec Endpoint Protection categorizes types of risks. The Malware category includes a subcategory called Virus. Macro and non-macro virus categories were included in earlier versions of the product. Macro and non-macro viruses are now detected as part of the Virus subcategory.

Security risks include spyware, adware, and other applications that can put a computer at risk. The Security risks subcategories change dynamically over time as Symantec gets new information about risks.

## **What is Shared Insight Cache?**

The Symantec Endpoint Protection Shared Insight Cache eliminates the need to scan the files that Symantec Endpoint Protection has determined are clean. When Symantec Endpoint Protection scans a file for threats and determines it is clean, the client submits information about the file to Shared Insight Cache. When another client subsequently attempts to scan the same file, the client can query Shared Insight Cache to determine if the file is clean. If the file is clean, the client can bypass virus scanning on that particular file. If the file is not clean, the client scans the file for viruses and submits those results to Shared Insight Cache.

Symantec uses the Shared Insight Cache feature in virtual infrastructures only.

[About Shared Insight Cache](#)

## **SONAR**

SONAR is the real-time protection that detects potentially malicious applications when they run on your computers. SONAR uses heuristics as well as reputation data to detect emerging and unknown threats. SONAR provides "zero-day" protection because it detects threats before traditional virus and spyware detection definitions have been created to address the threats.

## **What is Virtual Image Exception?**

Administrators leverage base images to build virtual machines for their virtual desktop infrastructure (VDI) environment. The Symantec Virtual Image Exception tool lets your clients bypass the scanning of base image files for threats.

---

Bypassing some files reduces the resource load on disk I/O. It also improves CPU scanning process performance in your VDI environment.

Before you enable this feature in Symantec Endpoint Protection Manager, first run the Virtual Image Exception tool against the base image files. The Virtual Image Exception tool marks the base image files by adding an attribute. If the file is modified, this attribute is removed. This tool is located in the /Virtualization/VirtuallImageException folder on the Symantec Endpoint Protection Tools installation file.

This feature is disabled by default. Enable the feature so that when your client starts to scan a file, it looks for this attribute. If the base image file is marked and remains unchanged, the client skips scanning the file.

**NOTE**

Symantec Endpoint Protection supports the Virtual Image Exception tool for both managed clients and unmanaged clients, but not its use in a physical environment. It cannot be used on non-fixed drives such as mapped network drives, CD/DVD drives, USB drives, and so on.

---

## Product Dialog Help

---

Reference information about settings on the dialog boxes

Use this section to browse through all the Help topics for the Symantec Endpoint Protection Manager dialog boxes.

### Logs

#### Basic filter settings for all logs and quick reports

You can use the default filter to view a log or quick report, or you can configure the filter options to limit the data view. You can save a filter that you have customized so that you can use it in the future.

The filter option fields are not case-sensitive. Some fields accept wildcard characters. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (\*), which matches any string of characters.

**Table 221: Basic filter options for all logs and quick reports**

Option	Description
<b>Log type</b> or <b>Report type</b>	Displays the log name or report name.
<b>Log content</b> or <b>Select a report</b>	Specifies the particular log or quick report that you want to view. Some logs or reports have more than one type.
<b>Use a saved filter</b>	Specifies the filter that you want to use to create the view. You can use the default filter or a custom filter that you have named and saved for viewing audit information.
<b>Time range</b>	Specifies the time range of events that you want to view in the log. For example, you can select <b>Past week</b> or <b>Past year</b> . <b>Note:</b> If you choose <b>Set specific dates</b> , you must set a <b>Start date</b> and an <b>End date</b> .

#### Basic options for all logs

[Options in all logs](#) describes the options that are available in the log window after you view one of the logs.

**Table 222: Options in all logs**

Option	Description
<b>Auto-refresh</b>	Specifies the rate at which this log refreshes.
<b>Back</b>	Returns to the log filter.
<b>Export</b>	Exports the log data in this filtered list to a comma-separated file.
<b>Details</b>	Displays the details about the selected entry.
<b>View Applied Filters</b>	Provides a view of the filters that you have applied to the log.

#### Common additional filter settings for all logs and quick reports

[Most common additional settings for all logs and quick reports](#) lists the most common filter settings that logs and reports use.

**Table 223: Most common additional settings for all logs and quick reports**

Option	Description	Log or report
<b>Event type</b>	Includes the component or action that triggered the event that you want to view.	All
<b>Severity</b>	Displays the minimum severity level of the events that you want to view. The setting filters the display to show only the specified severity level and above. For example, if you select <b>Major</b> , both the major and the critical events appear.	Application and Device Control, Compliance, Network and Host Exploit Mitigation, System
<b>Operating system</b>	Includes only those computers with this operating system.	Device Control, Compliance, Computer Status, Network and Host Exploit Mitigation, SONAR, Risk, Scan
<b>Site</b>	Includes the local site or the remote site that you want to view information about. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters. You can also click the dots to select from a list of known sites.	Audit, Application and Device Control, Compliance, Computer Status, Network and Host Exploit Mitigation, System
<b>Domain</b>	Includes the domain that you want to view information about. This field accepts a comma-separated list as input. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters. You can also click the dots to select from a list of known domains.	All
<b>Group</b>	Specifies the group that you want to view information about. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters. You can also click the dots to select from a list of known groups.  <b>Note:</b> Because all groups are subgroups of the default parent group, when this filter searches for groups, it searches hierarchically starting with the name of the default group. Unless the name of your group starts with the same letter, you should precede the search string with an asterisk when using wildcards.  <b>Note:</b> For example, if you have a group named Purchasing, and you type p* into this box, no group is found and used in the view. To find a group named Purchasing, you need to use *p* instead.	All but Audit
<b>Server</b>	Specifies the management server that you want to view information about. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters. You can also click the dots to select from a list of known servers.	All
<b>Computer</b>	Includes the computer that you want to view information about. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters. You can also use a comma-separated list as input.	Application and Device Control, Compliance, Computer Status, Network and Host Exploit Mitigation, SONAR, Risk, Scan
<b>User</b>	Includes the user names that you want to view information about.	All

Option	Description	Log or report
<b>IP address</b>	Includes the IP address of the computer that you want to view information about. When you want to filter logs or reports by using an IP address, use the IP address that appears in the Computer Status log view. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters. You can also use a comma-separated list as input.  <b>Note:</b> If you export the log the IP address might appear blank rather than using the x.x.x.x format. A blank IP address indicates that the risk was detected on the management server, rather than a remote computer.	Application and Device Control, Compliance, Computer Status, Network and Host Exploit Mitigation, Scan
<b>Remote IP address</b>	Specifies the remote host that you want to view information about. This field supports host names only, and not IPv4 or IPv6 addresses. It does validate whether or not the host name is correct.	Compliance, Network and Host Exploit Mitigation,
<b>Remote host</b>	Specifies the remote host that you want to view information about.	Compliance, Network and Host Exploit Mitigation,

[Viewing logs](#)

## Audit log and quick reports

The Audit log and quick report contain information about policy modification events.

The Audit report has one report type, **Policies Used**.

[Common additional filter settings for all logs and quick reports](#)

**Table 224: Additional Settings filter options for views of the Audit log**

Option	Description
<b>Policy name</b>	Specifies the name of the policy that you want to view information about. This field accepts a comma-separated list as input. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters.
<ul style="list-style-type: none"> <li>• <b>Event type</b></li> <li>• <b>Domain</b></li> <li>• <b>Site</b></li> <li>• <b>Server</b></li> <li>• <b>User</b></li> </ul>	For information on these settings: <a href="#">Common additional filter settings for all logs and quick reports</a>

[Basic options for all logs](#)

[Basic filter settings for all logs and quick reports](#)

## Compliance log and quick report

The **Client Host Integrity** log and quick report tracks the details of Host Integrity checks on the clients.

For some of the fields, you can use the wildcard character question mark (?), which matches any one character, and the asterisk (\*), which matches any string of characters. You can also click the dots to select from a list of known sites.

[Client Host Integrity log > Additional Settings](#)

[Compliance quick reports](#)



**Table 225: Client Host Integrity log > Additional Settings**

Option	Description
<ul style="list-style-type: none"> <li>• <b>Event type</b></li> <li>• <b>Operating system</b></li> <li>• <b>Severity</b></li> <li>• <b>Site</b></li> <li>• <b>Domain</b></li> <li>• <b>Group</b></li> <li>• <b>Server</b></li> <li>• <b>Computer</b></li> <li>• <b>User</b></li> <li>• <b>IP address</b></li> <li>• <b>Remote host</b></li> <li>• <b>Remote IP address</b></li> </ul>	<p>For information on these settings:  <a href="#">Common additional filter settings for all logs and quick reports</a></p>
<b>Protocol</b>	Specifies the protocol that you want to view information about. For example, you can select <b>TCP</b> or <b>ICMP</b> .
<b>Direction</b>	Specifies the traffic direction that you want to view information about.

**Table 226: Compliance quick reports**

Option	Description
<b>Host Integrity Status</b>	<p>Displays the clients that have passed or failed the Host Integrity check that runs on their computer.</p> <ul style="list-style-type: none"> <li>• <b>Passed</b> The client is installed and has a valid UID and passed the policy check and Host Integrity check.</li> <li>• <b>Failed</b> The client is installed and has a valid UID but failed the policy check and Host Integrity check.</li> </ul>
<b>Clients by Compliance Failure Summary</b>	Use this report to see the general reasons for control failure events, such as antivirus, firewall, or VPN.
<b>Compliance Failure Details</b>	Displays the failure rate of the individual checks that comprise a Host Integrity requirement. Provides more details than the <b>Clients by Compliance Failure Summary</b> . For example, it displays the clients that do not have antivirus installed separately from those that have out-of-date virus definitions.
<b>Non-compliant Clients by Location</b>	Use this report to see if some locations have more compliance problems than the others.

## Application and Device Control logs and quick reports

Application and Device Control logs and quick reports contain information about events where some type of behavior was blocked. Information includes items such as event times and types, actions taken, domains, hosts, rules, and caller processes.

Information is collected about application control and Tamper Protection, and about the hardware behavior and the software behavior that the Device Control technology detects.

### NOTE

Two log entries might appear in the Control log for a single event. For example, two entries might appear if an application reads and then tries to write a file. Two entries also appear if an application writes and then tries to delete a file. Also, the events that appear in the Control log might show a file size as 0 bytes rather than the

actual file size. Typically, the file size appears as 0 bytes when the application control rule triggers before a process creates or writes a file.

[Common additional filter settings for all logs and quick reports](#)

**Table 227: Additional filter options for the Application Control log and report and the Device Control log and report**

Option	Description
<ul style="list-style-type: none"><li>• <b>Severity</b></li><li>• <b>Event type</b></li><li>• <b>Operating system</b></li><li>• <b>Site</b></li><li>• <b>Domain</b></li><li>• <b>Group</b></li><li>• <b>Server</b></li><li>• <b>Computer</b></li><li>• <b>User</b></li><li>• <b>IP address</b></li></ul>	For information on these settings: <a href="#">Common additional filter settings for all logs and quick reports</a>
<b>Test mode</b>	Displays the events based on the mode that the policy is set at. Click <b>Yes</b> for <b>Test (log only)</b> mode and <b>No</b> for <b>Production</b> mode. <b>No</b> displays only information about the computers that are in <b>Production</b> mode and not <b>Test (log only)</b> mode. This option is available only for the <b>Application Control</b> log.
<b>Action</b>	Specifies the type of action that you want to view information about. For example, you can select <b>Block</b> or <b>Continue</b> . This option is available only for the <b>Application Control</b> log.
<b>File size</b>	Specifies the size of the file that application control detected. You can choose to view information about all the files or only files that are less than or greater than the specified size.
<b>Caller process</b>	Displays the process or application that triggers the event. For example, suppose that you create a rule to block programs from writing to a folder. If you then try to save a document to that folder, an event is logged where winword.exe is the caller process. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters. You can also use a comma-separated list as input. This option is available only for the <b>Application Control</b> log.

[Options in the Application and Device Control log window](#) describes the options that are available in the log window after you view one of the logs.

**Table 228: Options in the Application and Device Control log window**

Option	Description
<b>Action</b>	To add the selected process to the Exceptions policy so that the client does not scan it, click <b>Add Process to Exception Policy</b> , and then click <b>Start</b> .

**Table 229: Application and Device Control quick reports types**

Option	Description
<b>Top Groups With Most Alerted Application Control Logs</b>	Specifies the minimum severity level of the events that you want to view. The setting filters the display to show only the specified severity level and above. For example, if you select <b>Major</b> , both the major and the critical events appear.
<b>Top Targets Blocked</b>	This option is available only for the <b>Top Groups With Most Alerted Application Control Logs</b> report and the <b>Top Targets Blocked</b> report.
<b>Top Devices Blocked</b>	This option is available only for the <b>Top Devices Blocked</b> report.

[Basic options for all logs](#)

[Basic filter settings for all logs and quick reports](#)

## Computer Status logs and reports

The Computer Status logs and reports contain information about the operational status of the computers in your network, such as which computers are infected or the latest definitions update. You can also run some commands from the Computer Status logs.

### NOTE

The Computer Status log might include a report icon that you can click to view more information about a Power Eraser analysis.

For the **Time range**, you can configure **Set specific dates > Checked in since**. This option specifies that you want to see all entries that involve a computer that has not checked in with its server since this date and time.

**Table 230: Additional Settings > Standard options in the Computer Status log and quick report**

Option	Description
<b>Definition date</b>	Includes only those computers with a virus definition date later than the specified date, or a specified version. The specific virus definitions versions that exist in your database appear in this list as choices. A database maintenance task purges them periodically so that the number of versions that appears in this list does not grow infinitely large.
<b>Product version</b>	Looks for the computers that have an older client than the specified client version(s).
<b>Policy version</b>	Includes only those computers with this policy version.
<b>Service pack</b>	Includes only those computers with this service pack.
<b>IPS version</b>	Includes only those computers with the specified version(s) of intrusion prevention signatures.
<b>Last scan time older than</b>	Specifies to include all computers whose last scan was performed before this time. For example, you can select <b>Past 24 hours</b> or <b>Past month</b> .
<ul style="list-style-type: none"> <li>• <b>Site</b></li> <li>• <b>Domain</b></li> <li>• <b>Group</b></li> <li>• <b>Server</b></li> <li>• <b>Computer</b></li> <li>• <b>User</b></li> <li>• <b>IP address</b></li> <li>• <b>Operating system</b></li> </ul>	For information on these settings: <a href="#">Common additional filter settings for all logs and quick reports</a>

Option	Description
<b>Online status</b>	<b>Online</b> includes only those computers that are connected to a management server. <b>Offline</b> includes only those computers that are not connected a management server.

[What are the commands that you can run on client computers?](#)

**Table 231: Additional Settings > Compliance options in the Computer Status log and quick report**

Option	Description
<b>Host Integrity status</b>	Specifies whether the Host Integrity check succeeded or failed on the client computer.
<b>Host Integrity reason</b>	Specifies that you only want to see information about the computers that have this reason for their current Host Integrity status. For example, you can look at the computers where the reason is that the location changed.
Protection check boxes	Click the check boxes to display the client computers that have the specified protections disabled. <b>Infected only</b> displays only the computers that have an infection. <b>Trusted Platform Module installed</b> A Trusted Platform Module device

[Basic options for all logs](#)

[Basic filter settings for all logs and quick reports](#)

[Viewing system protection](#)

## Deception logs and reports

The **Deception** logs and reports contain information about any activity that the clients send back to Symantec Endpoint Protection Manager as the result of deceptor activity. A deceptor is designed to look like it is interesting to an attacker. However, it only sends events back to the client and to Symantec Endpoint Protection Manager to indicate that it has been attacked.

Deception is a set of tools that you use to present to a potential attacker what appears to be desirable data and an attack vector. You use these tools to quickly detect and stop infiltration attempts.

- [Actions to take on events in the Deception logs](#) displays the actions you can take on clients after you click **View Log**.
- [Deception reports](#) displays the quick reports and scheduled reports for deceptor activity.

**Table 232: Actions to take on events in the Deception logs**

Option	Description
<b>Place client(s) in Quarantine</b>	Moves the clients that you believe that are compromised in some way into the Quarantine.
<b>Place client(s) from Quarantine</b>	Removes the clients from the Quarantine. Use this option if either the attack was neutralized or because you quarantined the client in error.

**Table 233: Deception reports**

Summary	Description
<b>Top Machines with Deception Activity</b>	Displays the top client computers that get hit by attacker activity, as indicated by events from deceptors on the given computers. A deceptor consists of artifacts such as files that are delivered to client computers. When an attacker touches an artifact, the artifact triggers an event. By design, the artifacts are hidden from the everyday user, but are interesting to an intruder.
<b>Top Processes with Deception Activity</b>	Displays the caller processes that attackers use to trigger deception events. For example, if ping.exe was used to trigger the Network Lookup (DNS) Deceptor, then ping.exe is the caller process.
<b>Top Users with Deception Activity</b>	Displays the users that get hit by attacker activity the most, based on events from deceptors on the client computers the users use.
<b>Top Deceptors Triggered</b>	Displays which deceptors that the attackers touched the most.

[Basic options for all logs](#)

[Basic filter settings for all logs and quick reports](#)

## Network and Host Exploit Mitigation logs and quick reports

The Network and Host Exploit Mitigation logs and reports contain information about attacks on the firewall, firewall traffic and packets, and intrusion prevention. The logs also contain information about Memory Exploit Mitigation.

As of version 14.2, IPv4 and IPv6 are supported for references to IP. For earlier versions, only IPv4 is supported.

### NOTE

The filter option fields that accept wildcard characters and search for matches are not case-sensitive. The ASCII asterisk character is the only asterisk character that can be used as a wildcard character.

[Additional filter settings for the Network and Host Exploit Mitigation logs and reports](#) describes the additional filter settings for logs and reports.

**Table 234: Types of Network and Host Exploit Mitigation logs**

Option	Description
<b>Attacks</b>	Available information includes time, attack type, domain, group, computer, and client user name. Additional information available includes the severity; the direction and protocol; the local host IP/remote host IP, the location; and the number.
<b>Traffic</b>	Available information includes time, event type, action, severity, direction, computer, local host IP/remote host IP, protocol, client user name, and number.
<b>Packets</b>	Available information includes time, event type, action, domain, direction, computer, local host IP, local port, and remote host IP.
<b>Memory Exploit Mitigation</b>	Available information includes time, signature ID, group, computer, application name, severity, local host ID, client user name, profile serial number, and location.

**Table 235: Additional filter settings for the Network and Host Exploit Mitigation logs and reports**

Option	Description
<ul style="list-style-type: none"> <li>Severity</li> <li>Event type</li> <li>Operating system</li> <li>Site</li> <li>Domain</li> <li>Group</li> <li>Server</li> <li>Computer</li> <li>IP address</li> <li>User</li> <li>Remote host</li> <li>Remote IP address</li> <li>Local IP address</li> </ul>	<p>For information on these settings:  <a href="#">Common additional filter settings for all logs and quick reports</a></p>
<b>Direction</b>	Specifies the direction that you want to view information about. For example, you can select <b>Inbound</b> or <b>Unknown</b> .
<b>Local port (or ICMP type)</b>	Specifies the local port or ICMP type that you want to view information about. This option is only available for the <b>Traffic</b> log.
<b>Local port</b>	For the <b>Packets</b> log, specifies the local port that you want to view information about. This option is only available for the <b>Packets</b> log.
<b>Blocked status</b>	Specifies the <b>Blocked</b> status that you want to view information about. This option is only available for the <b>Packets</b> log and the <b>Traffic</b> log.
<b>Protocol</b>	Specifies the protocol that you want to view information about. For example, you can select <b>TCP</b> or <b>ICMP</b> . This option is only available for the <b>Attacks</b> log and the <b>Traffic</b> log.
<b>Application Name</b>	Use this option to find which applications the Memory Exploit Mitigation techniques have blocked or terminated. Memory Exploit Mitigation logs only.
<b>Profile Serial Number</b>	Use the policy number to help find which policy has blocked or terminated an application. Memory Exploit Mitigation logs only.
<b>Location</b>	Use this option to find out which locations on the client computers had a higher or lower rate of exploit attacks. Memory Exploit Mitigation logs only.

[Basic options for all logs](#)

[Basic filter settings for all logs and quick reports](#)

## SONAR logs

The **SONAR** logs contain information about the threats that SONAR detected. SONAR detects any behavior that is similar to known risk behavior to detect unknown viruses and security risks.

The SONAR quick reports are part of the Risk quick reports. The filter options that you can use to configure the reports are described in the Risk quick reports help.

[Risk logs and quick reports](#)

[Additional filter settings for the SONAR logs](#) describes the additional settings filter options for the logs.

[Action options in the SONAR logs](#) describes the options in the logs.

**Table 236: Additional filter settings for the SONAR logs**

Option	Description
<ul style="list-style-type: none"> <li>• <b>Event type</b></li> <li>• <b>Domain</b></li> <li>• <b>Group</b></li> <li>• <b>Server</b></li> <li>• <b>Computer</b></li> <li>• <b>IP address</b></li> <li>• <b>User</b></li> <li>• <b>Operating system</b></li> </ul>	<p>For information on these settings:  <a href="#">Common additional filter settings for all logs and quick reports</a></p>
<b>Action taken</b>	<p>Specifies the action taken that you want to view information about.</p> <p><b>You can select one of the following actions:</b></p> <ul style="list-style-type: none"> <li>• <b>All</b></li> <li>• <b>Access denied</b> View the events where the Auto-Protect portion of the client prevented a file from being created.</li> <li>• <b>Action invalid</b> View the events where the action was invalid. These risks may still be present on the computer.</li> <li>• <b>All actions failed</b> View the events where all the configured actions failed.</li> <li>• <b>Bad</b> View events where scan engine failure occurred for an unspecified reason. These risks may still be present on the computer.</li> <li>• <b>Cleaned</b> View the events where the software cleaned a virus from the computer.</li> <li>• <b>Cleaned by deletion</b> View the events where the action configured was "clean," but a file was deleted because that was the only way to clean it. For example, this action is generally needed for Trojan horse programs.</li> <li>• <b>Cleaned or macros deleted</b> View the events where a macro virus was cleaned from a file either by deletion or some other means. This action applies only to the events that have been received from computers running Symantec AntiVirus 8.x or earlier versions.</li> <li>• <b>Deleted or removed</b> View the events where the software deleted an object, such as a file or a registry key, to remove a risk.</li> <li>• <b>Excluded</b> View the events where users chose to exclude a security risk from detection. For example, this action can occur when a user is prompted for permission to terminate a process.</li> <li>• <b>Left alone</b> View the events where a risk was left alone. This action can occur if the first configured action was Leave alone. This action can also occur if the second configured action was Leave alone and the first configured action was not successful. This action may mean that a risk is active on the computer.</li> <li>• <b>No repair available</b> View the events where a risk was detected but a repair was not available to fix it.</li> <li>• <b>No repair available - Power Eraser recommended for repair</b></li> <li>• <b>Partially repaired</b> View the events where Symantec Endpoint Protection cannot completely repair the effects of a virus or security risk.</li> <li>• <b>Pending repair or Pending admin action</b> View the events where a user still needs to take action to complete the remediation of a risk on a computer. This action may occur if a user hasn't responded to a prompt to terminate a process.</li> <li>• <del><b>Process terminated</b></del></li> </ul>
	<ul style="list-style-type: none"> <li>View the events where a process was terminated.</li> <li>• <b>Process termination pending restart</b> View the events where a process needs to be terminated, but a restart of the computer is required to complete this action.</li> <li>• <b>Quarantined</b></li> </ul>

Option	Description
<b>Risk severity</b>	Specifies the severity category of risk that you want to view information about. <b>Unknown</b> Unknown risks are the risks that Symantec Security Response has not rated. <a href="#">For more details about severity, see the Symantec Security Response website.</a>
<b>Risk level</b>	Specifies the level of the risks that you want to view information about. SONAR categorizes risks as low, medium, or high.
<b>Risk name</b>	Specifies the risk names that you want to view information about. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters. This field also accepts a comma-separated list as input.
<b>Application</b>	Specifies the names of the applications that you want to view information about. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters. This field also accepts a comma-separated list as input.

[Action options in the SONAR logs](#) describes the exceptions you can add to the Exceptions policy from the log. Select the exception and click **Apply**.

**Table 237: Action options in the SONAR logs**

Option	Description
<b>Add folder to Exceptions policy</b>	Creates a SONAR folder exception for the folder where the file resides and does not automatically apply to subfolders. The exception applies only to SONAR.
<b>Allow application</b>	Creates an application exception with an action of <b>Ignore</b> . The file is identified by its hash. The exception applies to both SONAR and any virus and spyware scan.
<b>Block application</b>	Creates a SONAR application exception with an action of Quarantine. The file is identified by its hash.
<b>Trust Web domain</b>	Creates a trusted web domain exception that applies to the URL from which the file was downloaded. The exception only applies to files that Download Insight detected.

## Risk logs and quick reports

The Risk logs and reports include information about risk events on your server and their clients. Information available includes the event time, event actual action, user name, computer, risk name source, count, and file path.

Some scan actions in the logs and reports might recommend that you run Power Eraser on certain detections. In some logs and reports, you can filter on **Action taken** to check for these recommendations.

### NOTE

Power Eraser detections do not appear in Risk reports. Power Eraser is an aggressive scan that flags potential risks. Since the scan results might inflate the actual detection count, these detections are not included in the reports. The detections do appear in the logs, however, so that the administrator can take action on the potential risks.

[Actions](#) describes the options in the Risk logs.

[Basic Settings filter options for Risk quick reports](#) describes the filter options for a few of the quick reports.

The following table describes the Additional Settings filter options for the logs and quick reports.



**Table 238: Additional Settings filter options for views of the Risk logs and quick reports**

Option	Description
<b>Action taken</b>	<p>Specifies the action taken that you want to view information about.</p> <p><b>Select one of the following actions:</b></p> <ul style="list-style-type: none"> <li>• <b>All</b></li> <li>• <b>Access denied</b> View events where the Auto-Protect portion of Symantec Endpoint Protection prevented a file from being created.</li> <li>• <b>Action invalid</b> View events where the action taken was invalid. These risks may still be present on the computer.</li> <li>• <b>All actions failed</b> View events where both the primary action and the secondary action that is configured for the risk cannot be carried out for some reason.</li> <li>• <b>Bad</b> View events where scan engine failure occurred for an unspecified reason. These risks may still be present on the computer.</li> <li>• <b>Cleaned</b> View events where the software cleaned a virus from the computer.</li> <li>• <b>Cleaned by deletion</b> View events where the action configured was “clean,” but a file was deleted because that was the only way to clean it. For example, this action is generally needed for Trojan horse programs.</li> <li>• <b>Cleaned or macros deleted</b> View the events where a macro virus was cleaned from a file either by deletion or some other means. This action applies only to events that have been received from computers running Symantec AntiVirus 8.x or earlier versions.</li> <li>• <b>Deleted or removed</b> View the events where the software deleted an object, such as a file or a registry key, to remove a risk.</li> <li>• <b>Excluded</b> View the events where users chose to exclude a security risk from detection. For example, this action can occur when a user is prompted for permission to terminate a process.</li> <li>• <b>Left alone</b> Specifies the events where a risk was left alone. This action can occur if the first configured action is Leave alone. This action can also occur if the second configured action is <b>Leave alone</b> and the first configured action is not successful. This action may mean that a risk is active on the computer.</li> <li>• <b>No repair available</b> View the events where a risk was detected but no repair is available for the side effects of this risk.</li> <li>• <b>No repair available - Power Eraser recommended for repair</b> View the events where a scan cannot repair the side effects of certain detections. You should run Power Eraser on the computers where these events occur. After Power Eraser detects the threat, you must manually initiate the repair.</li> <li>• <b>Partially repaired</b> View the events where Symantec Endpoint Protection cannot completely repair the effects of a virus or security risk.</li> <li>• <b>Pending repair or Pending admin action</b> View the events where a user or administrator should take action to complete the remediation of a risk on a computer. For example, the <b>Pending repair</b> action might occur if a user hasn't responded to a prompt to terminate a process. <b>Pending admin action</b> occurs when Power Eraser requires the administrator to perform some action from the logs in the console.</li> <li>• <b>Process terminated</b> View the events where a process had to be terminated on a computer to mitigate a risk.</li> <li>• <b>Process termination pending restart</b> View the events where a computer needs to be restarted to terminate a process to mitigate a risk.</li> <li>• <b>Quarantined</b> View the events where Symantec Endpoint Protection quarantined a virus or a security risk.</li> <li>• <b>Restored</b> View the Power Eraser events that the administrator deleted but then chose to restore.</li> <li>• <b>Suspicious</b> View the events where a SONAR scan detected a potential risk but has not remediated it, either because it cannot or because you have configured it to only log detections.</li> </ul>

Option	Description
<b>Risk type</b>	Specifies the type of risk that you want to view information about. For example, you can select <b>Malware</b> , <b>Cookie</b> , or <b>Remote access</b> .
<ul style="list-style-type: none"> <li>• <b>Event type</b></li> <li>• <b>Domain</b></li> <li>• <b>Group</b></li> <li>• <b>Server</b></li> <li>• <b>Computer</b></li> <li>• <b>IP address</b></li> <li>• <b>User</b></li> <li>• <b>Operating system</b></li> </ul>	For information on these settings: <a href="#">Common additional filter settings for all logs and quick reports</a>
<b>Risk name</b>	If you know the name of the risk, then use this option. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters. It also accepts a comma-separated list as input.
<b>Application</b>	Specifies the name of the application that you want to view information about. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters. It also accepts a comma-separated list as input.

The following table describes the exceptions you can add to the Exceptions policy from the Risks log. Select the exception and click **Apply**.

**Table 239: Actions**

Option	Description
<b>Allow application</b>	Creates an application exception with an action of Ignore. The file is identified by its hash. The exception applies to both SONAR and any virus and spyware scan.
<b>Block application</b>	Creates a SONAR application exception with an action of Quarantine. The file is identified by its hash.
<b>Add file to Exceptions policy</b>	Creates an exception for the detected file so that virus and spyware scans no longer detect the file. The file is identified by its file path.
<b>Add folder to Exceptions policy</b>	Creates an exception for the folder where the detected files resides. Applies only to virus and spyware scans, not to SONAR scans. The exception does not automatically include subfolders.
<b>Trust Web domain</b>	Creates a trusted Web domain exception that applies to the URL from which the file was downloaded. The exception only applies to files Download Insight detected.
<b>Add risk to Exceptions policy</b>	Creates a known risk exception. Applies only to files that are detected as security risks (such as adware or spyware) that are known security risks.
<b>Add extension to Exceptions policy</b>	Creates an exception for the extension of the detected file. For example, if the file that you select has an extension of .doc, then DOC is added to the list of extensions that virus and spyware scans do not scan.
<b>Delete from Quarantine</b>	Removes the selected file from the client computers' quarantine.
<b>Download file that the client quarantined</b>	Downloads the files that the client detected as a risk, quarantined, and uploaded to the management server. Use this command to access the file for further analysis. Downloaded quarantined files support replication.
<b>Start Power Eraser Analysis</b>	Runs Power Eraser on the selected risks. Symantec Endpoint Protection sometimes recommends that you run a Power Eraser on a detected risk.
<b>Delete a risk that Power Eraser detected</b>	Removes the selected risks that Power Eraser detected on client computers. Use this command to manually remove risks that Power Eraser detected. Power Eraser does not remove risks automatically.
<b>Restore a risk that Power Eraser deleted</b>	Restores files that Power Eraser detected and that you or another administrator previously removed.

Option	Description
<b>Ignore a risk that Power Eraser detected</b>	Acknowledges the selected detections. Use this command after you have reviewed the selected detections and decided to leave them alone.

**Table 240: Basic Settings filter options for Risk quick reports**

Option	Description
<b>Group by</b>	Specifies the target that you want to see information about. For example, for <b>Risks Detections Count</b> , you can group by <b>Computer</b> . For example, for <b>New Risks Detected in the Network</b> , you can select <b>Group</b> or <b>User name</b> . For example, for <b>Risk Distribution Summary</b> , you can select <b>Risk name</b> or <b>Source</b> .
<b>Configure</b> ...	This option is only available for the <b>Comprehensive Risk Report</b> . By default, the <b>Comprehensive Risk Report</b> includes all of the distribution reports and the new risks. You can click this option to limit the data in this report.
<b>X-axis</b>	Specifies the variable you want to use on the X-axis of the 3D-bar graph. For example, you can select <b>User name</b> or <b>Server</b> .  <b>Note:</b> The graph displays the top five instances of this axis variable. If you selected computer as one of the variables and there are fewer than five infected computers, non-infected computers may appear in the graph.  This option is only available for the <b>Top Risk Detections Correlation</b> report.
<b>Y-axis</b>	Specifies the variable you want to use on the Y-axis of the 3D-bar graph. For example, you can select <b>Domain</b> or <b>Risk name</b> .  <b>Note:</b> The graph displays the top five instances of this axis variable. If you selected computer as one of the variables and there are fewer than five infected computers, non-infected computers may appear in the graph.  This option is only available for the <b>Top Risk Detections Correlation</b> report.

**Table 241: Additional filter settings for the Number of Notifications and the Number of Notifications Over Time quick reports**

Option	Description
<b>Acknowledged status</b>	Displays the notifications that you have read or not read.
<b>Notification type</b>	Specifies the type of notification that you want to view information about. For example, you can select <b>Client list change</b> or <b>New software package</b> .
<b>Created by</b>	Specifies that you want to view the notifications that have filters created by this user.
<b>Notification name</b>	Specifies the name of a particular notification that you want to view information about. You can click the ... option to select from a list of known notifications. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters. You can also click the dots to select from a list of notifications. By default, all notifications that have been created are included.

[Viewing risks](#)

## Scan logs and quick reports

The Scan logs and reports provide information about virus and spyware scan activity. Information available includes items such as the computer name, IP address, status, scan time, duration, and scan results.

[Additional Settings filter options for views of the Scan logs and quick reports](#) describes the additional settings filter options for logs.

[Options in the Scan logs](#) describes the options in the logs.

[Basic Settings filter options for the Scan quick reports](#) describes the basic settings filter options for quick reports.

[Additional Settings filter options for Scan quick reports](#) describes the additional settings filter options for quick reports.

**Table 242: Additional Settings filter options for views of the Scan logs and quick reports**

Option	Description
<b>Duration greater or equal</b>	Specifies that you only want to see information about scans where the scan length was equal to or greater than this value in seconds.
<b>Files scanned greater or equal</b>	Specifies that you only want to see information about scans where the number of files scanned was equal to or greater than this value.
<b>Risks greater or equal</b>	Specifies that you only want to see information about scans where the number of risks found was equal to or greater than this value.
<b>Files with detections greater or equal</b>	Specifies that you only want to see information about scans where the number of infections found was equal to or greater than this value.
<b>Status</b>	Specifies the completion status of a scan.
<b>Scan type</b>	Specifies whether to filter the report by events for manual scans, system or startup scans, Power Eraser, or all scans. You can also filter by the scans that run when new definitions arrive.
<ul style="list-style-type: none"><li>• <b>Domain</b></li><li>• <b>Group</b></li><li>• <b>Server</b></li><li>• <b>Computer</b></li><li>• <b>IP address</b></li><li>• <b>User</b></li><li>• <b>Operating system</b></li></ul>	For information on these settings: <a href="#">Common additional filter settings for all logs and quick reports</a>

[Options in the Scan logs](#) describes the options that are available in the log window after you view the log.

**Table 243: Options in the Scan logs**

Option	Description
<b>Detections</b>	Displays Risk log results for the selected scans. The difference between the Detections view and the Risk log is that the Detections view can indicate that scan results are pending. The Risk log does not indicate if any scan results are pending. The Detections view also cannot be filtered. For information about the options, see the Risk log help.

**Table 244: Basic Settings filter options for the Scan quick reports**

Option	Description
<b>Bin width</b>	Specifies the width of the bin to use to form the histogram. This option is only available for the <b>Scan Statistics Histogram</b> report. The default width is <b>60</b> .
<b>Number of bins</b>	Specifies the number of bins you want used to form the bars of the histogram. This option is only available for the <b>Scan Statistics Histogram</b> report. The default number of bins is <b>100</b> .

**Table 245: Additional Settings filter options for Scan quick reports**

Option	Description
<b>Duration greater or equal</b>	Specifies that only the scans where the scan duration exceeds this value are included in the report. This option is not available for the <b>Computers Not Scanned</b> report.
<b>Files scanned greater or equal</b>	Specifies that only scans where the number of files that were scanned is greater than or equal to this value are included in the report. This option is not available for the <b>Computers Not Scanned</b> report.
<b>Risks greater or equal</b>	Specifies that only scans where the number of risks that were found is greater than or equal to this value are included in the report. This option is not available for the <b>Computers Not Scanned</b> report.
<b>Files with detections greater or equal</b>	Specifies the number of infected files that you want to view information about. This option is not available for the <b>Computers Not Scanned</b> report. Limits the data to scans that found a number of infections that is greater than this value.
<b>Status</b>	Specifies the status of the scans that you want to view information about. For example, you can select <b>Completed</b> or <b>Canceled</b> . This option is not available for the <b>Computers Not Scanned</b> report.

## System logs and quick reports

The System logs contain information about the event times, event types, sites, domains, servers, and severity levels.

**The following System log types are available:**

- **Administrative**  
Available information includes items such as event time and event type; the domain, site, and server involved; severity; administrator; and description.
- **Client-Server Activity**  
Available information includes items such as event time and event type; the domain, site, and server involved; client; and user name.
- **Server Activity**  
Available information includes items such as event time and event type; the site and server involved; severity; description; and message.
- **Client Activity**  
Available information includes items such as event time, event type, event source, domain, description, site, computer, and severity.

[Additional Settings filter options for views of the System logs](#) describes the additional settings filter options for the logs.

**Table 246: Additional Settings filter options for views of the System logs**

Option	Description
<b>Error message</b>	Specifies the type of error message events you want to view. This option is only available for the <b>Administrative</b> log and <b>Server Activity</b> log.
<b>Client</b>	Specifies the client that you want to view information about. This option is only available for the <b>Client-Server Activity</b> log.
<b>Event source</b>	Specifies the software component that generated the event that you want to view information about. For example, the source can be <b>symlink</b> , the communications link to the server. This option is only available for the <b>Client Activity</b> log.
<ul style="list-style-type: none"> <li>• <b>Event type</b></li> <li>• <b>Severity</b></li> <li>• <b>Site</b></li> <li>• <b>Domain</b></li> <li>• <b>Server</b></li> <li>• <b>User</b></li> </ul>	For information on these settings: <a href="#">Common additional filter settings for all logs and quick reports</a>

Some of these fields accept a comma-separated list as input. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (\*), which matches any string of characters. You can also click the dots to select from a list of known sites.

**Table 247: Additional Settings filter options for System quick reports**

Option	Description
<b>Event type</b>	Specifies the type of event that you want to view information about. For example, for the <b>Top Clients That Generate Errors</b> report, you can select <b>Installation events</b> or <b>Policy events</b> . For example, for the <b>Top Servers That Generate Errors</b> report, you can select <b>Database maintenance events</b> or <b>Find unmanaged computers events</b> .
<b>Error message</b>	Specifies the type of error message that you want to see information about. This option is only available for the <b>Top Servers That Generate Errors</b> report and the <b>Database Replication Failures Over Time</b> report.
<b>Event source</b>	Specifies the software component that generated the event that you want to view information about. For example, the source can be <b>symlink</b> , the communications link to the server. This option is only available for the <b>Top Clients That Generate Errors</b> report.

The **Site Status** report has no Additional Settings filter options.

When administrators and limited administrators view reports, they see a subset of the information that system administrators see. The information includes the security summary, the total number of clients that have been installed, and the number of clients that have been online.

## Monitors: Summary tab

The **Summary** tab on the **Monitors** page displays concise, high-level summaries of important log data to give you an immediate picture of security status. All summaries display events for the time period that you configure for the **Home** page in the **Preferences** dialog box. The default value is to display events for the last 12 hours.

### NOTE

You can click any chart to see more details about the summaries in a new window.

**Table 248: Deception summaries**

Summary	Description
<b>Top Machines with Deception Activity</b>	Displays the top client computers that get hit by attacker activity, as indicated by events from deceptors on the given computers. A deceptor consists of artifacts such as files that are delivered to client computers. When an attacker touches an artifact, the artifact triggers an event. By design, the artifacts are hidden from the everyday user, but are interesting to an intruder.
<b>Top Processes with Deception Activity</b>	Displays the caller processes that attackers use to trigger deception events. For example, if ping.exe was used to trigger the Network Lookup (DNS) Deceptor, then ping.exe is the caller process.
<b>Top Users with Deception Activity</b>	Displays the users that get hit by attacker activity the most, based on events from deceptors on the client computers the users use.
<b>Top Deceptors Triggered</b>	Displays which deceptors that were touched the most.

**Table 249: Virus and Spyware Protection summaries**

Summary	Description
<b>Risk Distribution</b>	Displays the overall distribution of risks.
<b>New Risks</b>	Displays a table of newly found risks, the entity that detected them, and the computer that they were found on. A new risk is a risk that has been detected for the first time during the view's time period. As the summary view ages, the risks drop out of the list as the database purges log entries. You can configure the time period that is used for the summaries from the <b>Home</b> page in the <b>Preferences</b> dialog box. For example, suppose that you set your time period to the past 24 hours and your database to retain entries for 2 months. If the XYZ risk was last detected 6 months ago, it is no longer in an entry in the database. If Symantec Endpoint Protection detects XYZ within the past 24 hours, it appears here as a new risk.
<b>SONAR</b>	Displays the distribution of SONAR threats that have been found.
<b>Risk Distribution by Source</b>	Displays a summary of the risk distribution by the source of the risk.
<b>Risk Distribution by Group</b>	Displays a summary of the risk distribution by the groups.

**Table 250: Network and Host Exploit summaries**

Summary	Description
<b>Top Targets Attacked by Subnet</b>	Displays a summary of the top targets that have been attacked. You can select from the list box to organize the targets by groups, subnets, clients, or ports. You can click the pie chart to see more details in a new window.
<b>Attack Event Types</b>	Displays a summary of the types of security events that have occurred.
<b>Top Sources of Attack</b>	Displays a summary of the top sources of the attacks.
<b>Memory Exploit Mitigation Detections</b>	Displays a summary of the Memory Exploit Mitigation events.
<b>Security Events by Severity</b>	Displays the distribution of events by severity: Critical, Major, Minor, and Informational.

**Table 251: Compliance summaries**

Summary	Description
<b>Compliance Status Distribution</b>	Displays the clients that have failed the Host Integrity check that runs on their computer.
<b>Clients by Compliance Failure Summary</b>	This summary displays the failure rate of the overall requirement. For example, it displays a count of the unique workstations by the type of control failure event, such as antivirus, firewall, or VPN as a bar chart.
<b>Compliance Failure Details</b>	Displays the failure rate of the individual checks that comprise a Host Integrity requirement. Provides more details than the <b>Clients by Compliance Failure Summary</b> . For example, it displays the clients that do not have antivirus installed separately from those that have out-of-date virus definitions.

**Table 252: Site Status summary**

Summary	Description
<b>Site Status</b>	Displays the overall security health status of the site. You can click the status to see the full site status report.
<b>Top Error Generators By Server</b>	Displays a summary of the top servers that generated errors and warnings.
<b>Top Error Generators By Client</b>	Displays a summary of the top clients that generated errors and warnings.
<b>Replication Failures Over Time</b>	Displays a summary of the database replication failures that have occurred during the configured time period.

[Monitoring endpoint protection](#)

## Client Log Settings for group name

You can use this dialog box to perform the following tasks:

- To enable the uploading of log information from clients to the management server.
- To set size, time of retention, and damper options for the upload cache that is used on the clients

If some network computers do not connect for long periods of time, it may be useful to limit the size of the upload cache. These settings apply to all the clients in the group.

### NOTE

These settings apply only to the log entries that are kept in the upload cache. They do not affect the number of entries or size of the logs that the client keeps.

**Table 253: Group settings for client logs**

Option	Description
<b>Maximum Size</b>	Specifies the maximum size of the data that you want to upload in this log. The default value is 512 KB for the System, Security and Risk, and Traffic logs. The default value is 1024 KB for the Packet log and the Control log.
<b>Retain for</b>	Specifies the number of days that you want to keep data. The default value is 14 days.



Option	Description
<b>Upload to management server</b>	Specifies that you want the clients in this group to send this log up to the management server. The default value is to upload the logs.
<b>Damper period</b>	Specifies the amount of time you want the client to spend condensing similar log records in to a single record. The default value is 7200 seconds (2 hours).
<b>Damper idle</b>	Specifies the maximum amount of time you want a client to wait between the condensing of similar log records into single records. The default value is 10 seconds.
<b>Upload maximum size</b>	Specifies the maximum number of records that you want a client to upload to the manager at a time. The default value is 100 records.

You can view the information from the client logs from the console or by using a web browser.

**Table 254: Displaying information from client logs on the console**

Client log	Where to view the information in the console
<b>System Log</b>	View this information in the <b>System Client Activity</b> log.
<b>Security and Risk Logs</b>	View this information in the <b>Risk</b> log.
<b>Security Logs</b>	View this information in the <b>Application Control</b> log, the <b>Compliance &gt; Client Host Integrity</b> log, and the <b>Network and Host Exploit Mitigation &gt; Attacks</b> log.
<b>Traffic Log</b>	View this information in the <b>Network and Host Exploit Mitigation &gt; Traffic</b> log
<b>Packet Log</b>	View this information in the <b>Network and Host Exploit Mitigation &gt; Packets</b> log.
<b>Control Log</b>	View this information in the <b>Application Control</b> log and the <b>Device Control</b> log.

## Choose Power Eraser Type

You can select whether Power Eraser analysis should run with or without rootkit detection. You should run Power Eraser on the fewest number of computers possible. If you run the analysis on many computers at the same time, you might adversely affect the performance of your network.

### WARNING

You should only run Power Eraser after you have tried other methods of virus removal. Power Eraser is an aggressive analysis that is prone to false positives.

Client computers must be connected to the network so that Power Eraser can use reputation information from Symantec Insight.

**Table 255: Power Eraser options**

Option	Description
<b>Analyze without rootkit detection</b>	Runs a Power Eraser analysis without rootkit detection.
<b>Analyze with rootkit detection (requires a reboot)</b>	Runs Power Eraser with rootkit detection. Rootkit detection is an even deeper analysis that runs after a required restart. You should typically select this option for ELAM detections that require Power Eraser analysis. This option is not available for limited administrators who do not have privileges for restart options.

Option	Description
<b>Restart Options</b>	By default, the computer restarts immediately unless the user delays the restart for 30 minutes. You can change the time of the restart, whether or not the user is prompted, and the type of restart to perform. The restart options you configure here are for Power Eraser analysis only. When you manually remediate Power Eraser detections, Power Eraser uses the group restart options.

## Site/Server Properties

### Site Properties: LiveUpdate

This dialog box lets you control and configure how often to check for new updates and download them to Symantec Endpoint Protection Manager for distribution to the clients. You can also specify the type of content to update, the languages used, and the server from which to get the updates. Generally, only large networks implement different source servers for security and bandwidth optimization.

**Table 256: LiveUpdate settings**

Settings	Options and Descriptions
<b>LiveUpdate Source Servers</b>	Specifies the server that provides the updates to the site servers. You can add and edit the source servers.
<b>Disk Space Management for Downloads</b>	Specifies the disk space that is used to store LiveUpdate downloads. <ul style="list-style-type: none"> <li><b>Number of content revisions to keep</b> Specifies the number of LiveUpdate content revisions to keep in the database. <a href="#">Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager</a></li> </ul>
<b>Download Schedule</b>	Specifies the schedule LiveUpdate uses for downloads. You can edit the schedule for downloads.
<b>Platforms to Download</b>	Specifies the platforms for which to download content. You can edit the list of platforms to download.
<b>Content Types to Download</b>	Specifies the types of content files to download to Symantec Endpoint Protection Manager for distribution to the clients. You can edit the list of content types to download.
<b>Content to Download for Client Types</b>	Specifies the content sizes to download for your client types. You should select all the client types that are installed in your network. You can run cloud-enabled standard and embedded/VDI clients. These clients use compact content that includes only the latest definitions. You should also download full content for any dark network clients. Dark network clients are any clients that specifically run without access to the cloud. If your network includes legacy clients (12.1.x), you should also download legacy reduced-size content or standard-size content for those clients. <b>Warning!</b> You must include all client types and content types that you have installed in your network. Each content type applies to a specific client and version. For example, 12.1.x standard clients cannot use content for 14 standard clients.
<b>Languages to Download</b>	Downloads the product updates in the languages that you select. You do not need to select the language for definitions and other content, as these updates are downloaded automatically for all languages by default.

## Download LiveUpdate Content

You can download LiveUpdate content to the Symantec Endpoint Protection Manager server on demand. The content that you download resides on the server. You must update client computers to receive the content.

---

This page summarizes the download content that you selected on the LiveUpdate tab of the Site Properties page.

[How to update content and definitions on the clients](#)

## Languages to Download

Select the language for the product updates you want to download. This setting does not apply to other types of content, which are downloaded automatically for all languages by default.

To remove a language you have already added, re-add only the languages that you want.

In 14.3 RU2 and later, Symantec Endpoint Protection is translated into four languages only: French, Japanese, Brazilian Portuguese, and Spanish. For unsupported languages, such as Italian, the client language automatically upgrades to English, as long as you enable the **Upgrade to English if unsupported language is unavailable** option in the **Client Install Package**. If you do not enable this option, the clients with unsupported languages do not automatically upgrade.

## LiveUpdate Servers

This dialog box lets you select the location of the LiveUpdate server from which to update the Symantec Endpoint Protection server site.

**Table 257: LiveUpdate server options**

Option	Description
Use the default Symantec LiveUpdate Server	Uses the default Symantec LiveUpdate server to update the Symantec Endpoint Protection server site. The Symantec Endpoint Protection servers pull updates through your Internet gateway.
Use the Symantec LiveUpdate server for prereleased content	Uses the Symantec Early Adopter server. You select this option if you want to test upcoming engine updates before they are released. Symantec releases new updates about two weeks before they are released to the public.
Use a specified internal LiveUpdate Server	Uses an internal LiveUpdate server to update the Symantec Endpoint Protection server site. If you select this option, the LiveUpdate server must be installed and configured. The LiveUpdate server pulls updates through your Internet gateway.

## Add or Edit LiveUpdate Server

This dialog box lets you configure the Symantec Endpoint Protection Manager to download updates from an internal LiveUpdate server to Symantec Endpoint Protection Manager. You must have previously installed a LiveUpdate server.

**Table 258: LiveUpdate server options**

Setting	Description
Server name	The name of the server. This name appears when you run LiveUpdate.
Description	This box is optional. You can type the descriptive information that is related to the server. For example, you can type the name of the site.
URL	<ul style="list-style-type: none"><li>You use the HTTP or HTTPS method only. Type the URL for the server, such as: Domain name: <code>http://myliveupdateserver.com</code><ul style="list-style-type: none"><li>IPv4 address: <code>http://192.168.133.11/Export/Home/LUDepot</code></li><li>IPv6 address: <code>http://[fd00:fe32::b008]:80/update</code></li></ul></li></ul> <p><b>Note:</b> Support for the FTP method or the UNC method was removed in 14.3 RU1.</p>

Setting	Description
User name	The logon name that is associated with the server. If required, enter a user name, otherwise leave this box blank.
Password	The logon password that is associated with the server. If required, enter a password, otherwise leave this box blank.

## Platforms to Download

Lets you select the platforms to download LiveUpdate content for, Mac and Windows. You can download 32-bit or 64-bit content for Windows, or both.

## Download Schedule

Specifies the schedule to use for LiveUpdate downloads to the management server from Symantec.

**Table 259: LiveUpdate**

Settings	Description
<b>Frequency</b>	Specifies the frequency with which to run LiveUpdate to check for updates. For Symantec Endpoint Protection Manager, select <b>Continuously</b> to make the server check for updates at 15-minute intervals, but the server downloads updates only when new downloads are available. If you specify a frequency, the first time LiveUpdate runs is a random time between the current time and the current time plus the specified frequency.
<b>Start, End, Every</b>	The <b>Start</b> and <b>End</b> settings specify the time interval during which LiveUpdate can start an update to the site servers. You can also specify a day of the week. This option is available only for Daily and Weekly frequencies.
<b>Retry interval (in minutes   hours) and Retry window (in hours   days)</b>	Specifies when to retry running LiveUpdate if for some reason LiveUpdate failed to run or complete due to a network outage or some other problem. The window value and the interval value depend on the frequency that you select. These options are disabled if you select <b>Continuously</b> for <b>Frequency</b> .

## Full Definitions Download

### Prevent clients from downloading full definition packages

Use this setting to help lessen excessive network load if many clients request downloads of a full set of virus and spyware definitions from the management server. You should enable the setting when you receive a notification that too many clients requested the full set of definitions. Enabling this setting does not stop current downloads, but it does prevent any future downloads.

This setting is disabled by default.

#### **WARNING**

If you enable this setting, make sure that you let your clients get protection updates from a LiveUpdate server. Otherwise, your clients do not get any updates.

To help prevent network overloads, perform these additional tasks:

- Receive a notification if too many clients request full definitions from the management server.  
You set the conditions for this notification based on what constitutes an overload for your environment. To configure the notification, add a **Network load: requests for virus and spyware full definitions** notification condition.

---

### [Setting up administrator notifications](#)

- Let clients download definitions from a LiveUpdate server to get a smaller package.  
In a LiveUpdate Settings policy, click **Advanced Settings > Download smaller client installation packages from a LiveUpdate server**.

### [Mitigating network overloads for client update requests](#)

## Content to Download for Client Types

Content for the standard and embedded/VDI clients is cloud-enabled and includes only the latest virus and spyware definitions. These clients use the cloud to scan files with the full set of definitions. Symantec Endpoint Protection also provides a dark network installation for any clients that are not connected to the cloud and require the full set of definitions.

### [How to choose a client installation type](#)

If your network includes clients earlier than 14, you must download the reduced-size content and standard-size content for those legacy clients.

#### **WARNING**

You must download the appropriate content for the clients in your network. If you do not download the content that your installed clients require, the clients cannot get updates from the management server.

**Table 260: Content to Download for Client Types**

Option	Description
<b>Standard and embedded clients (reduced-size content)</b>	Downloads a compact set of cloud-enabled definitions to the management server for standard and embedded/VDI clients. Virus and spyware scans on these clients use the extended set of definitions in the cloud. 12.1.x standard or 12.1.6.x embedded clients cannot use this content.
<b>Dark network clients (standard-size content)</b>	Downloads the full set of definitions to the management server for dark network clients only. This content is not cloud-enabled.
<b>Legacy embedded clients (legacy reduced-size clients)</b>	Downloads reduced-size content to the management server for 12.1.6.x embedded/VDI clients only. Enabled by default when you migrate Symantec Endpoint Protection Manager from 12.1.x to 14.
<b>Legacy standard clients (legacy standard-size content)</b>	Downloads a full set of definitions to the management server for 12.1.x standard clients only. Enabled by default when you migrate Symantec Endpoint Protection Manager from 12.1.x to 14.

## Policies

### Overview

This page provides an overview for each policy. If required, you can assign this policy to specific locations in a group.

**Table 261: Policy overview options**

Tab	Description
Policy Name	<p>Provides the name and description for each policy.</p> <p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Policy name</b> Name of the policy. When you create a new policy, this text box is mandatory. The following characters are not allowed in the policy name: / \ * ? &lt; &gt;   : "</li> <li>• <b>Description</b> Description of the policy.</li> <li>• <b>Enable this policy</b> Enables a policy and assigns it to a location or group. Disable the policy if you want to set up the policy and download the settings to the client at a later time. Policies are enabled by default.  <b>Note:</b> You cannot disable a Virus and Spyware policy or a LiveUpdate policy.</li> <li>• <b>Created</b> The policy creator.</li> <li>• <b>Last modified</b> Date of the last policy modification.</li> </ul> <p>After you click <b>OK</b>, the new policy name and description appear in the policy list in each policy's main window.</p>
Used By	<p>Identifies the groups and locations to which this policy is applied.</p> <p>This tab appears when you edit a policy, not when you initially create one. After you assign the policy, the tab appears with the groups and locations. You can change the tree view to a list view.</p> <p><b>Note:</b> This tab does not appear for non-shared policies.</p>

Performing the tasks that are common to all policies

## Policy Components

You can add and modify the policy components that specific policies or other features use.

**Table 262: Policy components**

Component	Description
Scheduled Scan Templates	<p>A list of administrator-defined scheduled scans.</p> <p>This component is used by the Virus and Spyware Protection policies.</p>
Management Server Lists	<p>A list of management servers that clients can connect to.</p> <p>This component is used for client communication.</p>
File Fingerprint Lists	<p>A list of file fingerprint files. The client software uses a checksum tool that figures out an application's file fingerprint.</p> <p>This component is used by the Application and Device Control policies.</p>
Host Groups	<p>A list of hosts that can trigger a firewall rule. You can define the host by DNS domain, DNS name, IP address, IP range, MAC address, or subnet.</p> <p>This component is used by the Firewall policies.</p>
Network Services	<p>A list of ports and protocols that can trigger a firewall rule.</p> <p>This component is used by the Firewall policies.</p>

Component	Description
Network Adapters	A list of network adapters that can trigger a firewall rule. This component is used by the Firewall policies.
Hardware Devices	A list of hardware devices. You can add devices to the list. This component is used by the Application and Device Control policies. You use the policy to allow or block the devices that you select from the list.

## Policies

Use the Policies page to set up a security policy that is downloaded to all clients in selected groups or locations. The security policy can include one or more of several types of policies, which you can create and maintain from the Policies pane.

**Table 263: Policy types**

Policy type	Description
<b>Virus and Spyware Protection</b>	Provides the additional protection from viruses and security risks, and repairs the side effects of risks. The protection includes real-time scans of files and email, as well as scheduled scans and on-demand scans. You can also protect client computers against zero-day attack vulnerabilities in your network.
<b>Firewall</b>	Provides a customizable firewall that protects clients from intrusion and misuse by using firewall rules, traffic settings, and stealth settings.
<b>Intrusion Prevention</b>	Protects the client computer against intrusion attempts. You can create exceptions to IPS signatures, enable the intrusion prevention system, and enable intrusion prevention settings. In addition, you can import and create custom IPS signatures.
<b>Application and Device Control</b>	Controls the access to files and folders, registry keys, processes, and DLLs. The protection also allows or blocks access to the hardware devices that users plug in to the client.
<b>Host Integrity</b>	Defines, enforces, and restores the security of compliant and non-compliant computers.
<b>LiveUpdate</b>	Checks for and distributes content, component, and product updates to client computers.
<b>Exceptions</b>	Enables you to create exceptions for Windows, Mac, and Linux. Available exception types vary by operating system, and include virus and spyware scans, SONAR, and Tamper Protection.
<b>Memory Exploit Mitigation</b>	Stops vulnerability attacks on software using mitigation techniques such as DLL hijacking, heapspray mitigation, and Java exploit prevention.
<b>Network Traffic Redirection</b>	Integrates Symantec Web Security Service (WSS) functionality into Symantec Endpoint Protection. Network Traffic Redirection (NTR) automatically redirects all Internet traffic or just web traffic on the client to the Symantec WSS, where the traffic is allowed or blocked based on the WSS policies.

The policies you create are listed in each Policies page and include the following information:

- Name of the policy.
- Description of the policy.
- Number of locations or groups to which the policy is assigned.

You can view recent changes to the policy, including:

- Description of the change.
- Date and time of the change.
- Name of the administrator who modified the policy.

When you select a policy, you can perform a number of tasks. You can access these tasks either by right-clicking each policy page or by clicking the list under **Tasks**. You can use these commands to add, edit, delete, assign, withdraw, replace, import, export, and copy policies.

Under **Tasks**, you can also search for the applications that each client runs. You can use the query tool to find application information to use when you create policies for Firewall, Application and Device Control, or Host Integrity.

The policies on the **Policies** page are shared, and you can assign the policies to any location.

Use the Policies page to set up a security policy that is downloaded to all clients in selected groups or locations. The security policy can include one or more of several types of policies, which you can create and maintain from the Policies page.

## Withdraw the type of Policy

You withdraw a policy from a group or a location when you want to delete it or you save it to use for another time. You must withdraw a policy from every group and location before you can delete it. This action does not delete the selected policy.

To withdraw a policy, uncheck the policy from the groups and locations to which it no longer applies.

[Assigning a policy to a group or location](#)

## Replace the policy

You can replace one policy with another if more than one policy exists for that policy type.

**Table 264: Replacement of a policy**

Option	Description
Old type of Policy	Lists the policy that you want to replace.
New type of Policy	Enables you to select the new policy that you want to assign to a group and location.
Groups tree view	Lists the groups for which you can replace a policy.
Replace	Replaces the old policy with the new policy for selected groups and locations.

## Search for Applications

You can find specific information about the applications that the clients run. You can search the list of learned applications that the client sends to the management server. You can search for the applications that a specific user or client computer runs. You can also search on the application's characteristics, such as the file name.

You can use this information to find out what applications your users are running. Learned applications can help you set up policy features that control or detect applications, such as firewall or application and control rules.



**Table 265: Search for applications options**

Option	Description
Search for applications in	Specifies a group and a location that contain the clients that you want to search the list of the applications for.
Browse	Displays the Select Group or Location dialog box, where you can select a parent group, a subgroup, or a location within a group.
Search subgroups	Searches for the locations and the subgroups of the group you selected in the <b>Select Group or Location</b> dialog box.
Search Criteria	Searches for an application that is based on the following criteria: <ul style="list-style-type: none"> <li>Based on client/computer information <ul style="list-style-type: none"> <li>Searches for an application that runs on a particular client computer</li> </ul> </li> <li>Based on applications <ul style="list-style-type: none"> <li>Searches on characteristics of a particular application.</li> </ul> </li> </ul>
Search Field	<p>If you selected the client-computer information option, the following criteria appear:</p> <ul style="list-style-type: none"> <li>BIOS version <ul style="list-style-type: none"> <li>A string</li> </ul> </li> <li>Computer Domain Name</li> <li>Computer Name</li> <li>IP Address</li> <li>Memory</li> <li>Operating System</li> <li>Operating System Language</li> <li>Processor Clock <ul style="list-style-type: none"> <li>Number up to 20 characters long</li> </ul> </li> <li>Processor Number <ul style="list-style-type: none"> <li>A number up to 10 characters long</li> </ul> </li> <li>Processor Type</li> <li>Service Pack <ul style="list-style-type: none"> <li>String</li> </ul> </li> <li>TPM Device</li> <li>Total Disk Space</li> <li>User Domain Name</li> <li>User Name <ul style="list-style-type: none"> <li>The format of the Value field can change, depending on the criteria that you select in the drop-down list.</li> </ul> </li> </ul> <p>If you selected the applications option, the following criteria appear:</p> <ul style="list-style-type: none"> <li>Application Description</li> <li>Application Fingerprint</li> <li>Application Name</li> <li>Application Path</li> <li>Application Size <ul style="list-style-type: none"> <li>Number up to 20 characters, in bytes</li> </ul> </li> <li>Application Version <ul style="list-style-type: none"> <li>String</li> </ul> </li> <li>Last Modified Time <ul style="list-style-type: none"> <li>Enter in the format mm/dd/yyyy hour:minutes:seconds</li> </ul> </li> </ul> <p>The format of the Value field can change, depending on the criteria that you select in the drop-down list.</p>

Option	Description
Comparison Operator	<p><b>Lists the following operators to specify a value:</b></p> <ul style="list-style-type: none"> <li>• = Equal to</li> <li>• != Not equal to</li> <li>• &gt; Greater than</li> <li>• &lt; Less than</li> <li>• &gt;= Greater than or equal to</li> <li>• &lt;= Less than or equal to</li> <li>• LIKE LIKE matches a partial entry. LIKE places a wildcard character (% or ?) at both the beginning and the end of the string that you enter. The query then locates any strings that begin with, end with, or contain the value that you entered.</li> </ul>
Value	<p>Specifies the value for the Search Field criteria.</p> <p>The Value field filters your results. If you do not specify a value, you may get a large set of results that can take a long time to search through.</p> <p>You can use the following criteria to specify the value:</p> <ul style="list-style-type: none"> <li>• Most values are strings</li> <li>• Strings are not case sensitive</li> </ul> <p>The criteria you enter in the Search Field may display a preset format. For example, if you select an IP address, an IP address format is displayed.</p>
Search and Stop	Starts and stops the search.
Export	Saves the search results in a text or comma delimited (.csv) file.
Clear All	Clears the search results from the Query Results table.
Previous and Next	Scrolls through rows of results by page.
View Details	Displays the information about an application or a client computer in a dialog box rather than in a row. You can copy and paste the information from the View Details dialog box, but you cannot modify it.

## View Details

Use the View Details dialog box to view each field that the client records about the selected learned application. You can view the client details as well as the application details. The client details include the computer name, description, domain, and location name.

## Exceptions Policy

You can view and customize information about an Exceptions policy.

Use the **Policy Name** tab to customize the name and description for the policy. On the **Used By** tab you can view the groups that currently use the policy. You can view groups in a tree view or a list view.

**Table 266: Overview options**

Option	Description
<b>Policy name</b>	Enter a name for the policy that contains exceptions you want to apply.
<b>Description</b>	Type a description for the policy.
<b>Enable this policy</b>	Use this option to enable or disable the policy. You might want to temporarily disable exceptions on your client computers without removing each configured exception.
<b>Created</b>	Shows the name of the administrator who created the policy.
<b>Last modified</b>	Shows the date and time that the policy was last modified.

## Exceptions

Use this page to add, edit, or view exceptions for virus and spyware scans, SONAR, and Tamper Protection. You can also exclude applications from application and device control.

You can configure exceptions for Windows, Mac, and Linux clients. Some exceptions are not supported on some client operating systems.

Any exception that you include in the policy applies to all scans of the same type. For example, you might create an exception to exclude a security risk. The client software then excludes the security risk from all virus and spyware scans on the computers that use the policy.

**Table 267: Exceptions**

Field	Description
<b>Exception Item</b>	Shows the file name, folder name, application name, or Web domain that should be excluded from a scan. For application exceptions, the file fingerprint appears with an indication for whether the file hash uses SHA-1 or SHA-2.
<b>Platform</b>	Displays the platform to which the exception applies. Exceptions are platform-specific.
<b>Exception Type</b>	Specifies the type of exception.
<b>Action</b>	Displays the action that Symantec Endpoint Protection takes on the file, folder, or Web domain.
<b>Exception Details</b>	Provides more information about a selected exception.

## Exceptions: Client Restrictions

Use this page to specify restrictions for the types of exceptions that client computer users can add. By default, users can create any type of exception. If you deselect an exception type, the user cannot create any exception of that type.

### NOTE

Users cannot configure Tamper Protection exceptions.

## Application to Monitor

Use this dialog box to specify a file name for an application that Symantec Endpoint Protection should learn. This type of exception forces Symantec Endpoint Protection to learn an application. It does not affect how scans detect the file.

When Symantec Endpoint Protection learns the application, the detections appear in the **Application Exception** dialog box. Then you can create an exception to configure an action for the specified process.

The application that you specify is learned even if you turn off application learning.

---

## NOTE

Because file names are not unique, multiple applications might use the same file name. The **Application Exception** dialog box shows the file fingerprint that is preceded by a 1 or a 2 to indicate SHA-1 or SHA-2.

Type the name of the application that you want to force Symantec Endpoint Protection to learn in the **Application to Monitor** text box.

You can also edit an existing exception by editing or retyping the name of the process.

## Application Exception

Use this dialog box to specify an action for an application that you monitor or that users download. Depending on the action that you specify, Symantec Endpoint Protection applies the action when it detects the application or the application runs.

Use the **Add an Application by Fingerprint** option to add the hash value of the application. This method lets you add an exception quickly (as of 14.3 RU1)

Use the **Application an Application to Monitor** option to choose an application that you want the client to monitor. When Symantec Endpoint Protection learns the application, the application name appears in the **Application Exception** dialog and you can configure an action for the application. This process can take up to a few hours to complete. Because file names are not unique, multiple applications might use the same file name. The list shows the application's file fingerprint that is preceded by a 1 or a 2 to indicate SHA-1 or SHA-2.

**Table 268: Application to Monitor Exception**

Option	Description
<b>View</b>	<p>You can filter the applications by the following types:</p> <ul style="list-style-type: none"> <li>• <b>All</b> Shows all detected applications.</li> <li>• <b>Watched Applications</b> The applications that you specified as Application to Monitor exceptions.</li> <li>• <b>User-allowed Applications</b> User-allowed applications are the applications that users choose to allow when they try to download files.</li> </ul> <p><b>Note:</b> If you change an application's file name and configure an exception to monitor that application with its new file name, the application does not appear in the watched applications list with its new name. Instead the application appears in the unfiltered list with its original name.</p>
<b>Action</b>	<p><b>You can specify any of the following actions:</b></p> <ul style="list-style-type: none"> <li>• <b>Ignore</b> Excludes the application from detection by future scans.</li> <li>• <b>Log only</b> Adds an entry in the scan logs when the process is detected. This action is the default action.</li> <li>• <b>Quarantine</b> Quarantines the application when it tries to run.</li> <li>• <b>Terminate</b> Stops the application from running but does not remove it from the computer.</li> <li>• <b>Remove</b> Stops the application and removes it from the computer.</li> </ul> <p><b>Note:</b> The <b>Quarantine</b>, <b>Terminate</b>, and <b>Remove</b> actions apply when the specified application runs. The <b>Ignore</b> and <b>Log only</b> action apply when Symantec Endpoint Protection detects the application.</p>

## Application Exception by Fingerprint

Use this dialog box to add an application exception based on an application's hash value. This method is faster than using an application to monitor, which first adds the application to the monitor list. The client then sends the hash value and other application information to the management server. You can then add that application as an exception. This process can take up to a few hours to complete.

This type of exception forces Symantec Endpoint Protection to learn an application. It does not affect how scans detect the file.

This feature is available as of 14.3 RU1.

**Table 269: Application exception based on the file fingerprint**

<b>Application fingerprint</b> (required)	Add the application's HASH value using the SHA-256 algorithm.
<b>Application name</b> (optional)	Use this field to distinguish between multiple applications that have similar names.

<b>Specify the action to take on the this application</b>	<ul style="list-style-type: none"> <li>• <b>Ignore:</b> Excludes the application from detection by future scans. This action is the default action.</li> <li>• <b>Log only:</b> Adds an entry in the scan logs when the process is detected.</li> <li>• <b>Quarantine:</b> Quarantines the application when it tries to run.</li> <li>• <b>Terminate:</b> Stops the application from running but does not remove it from the computer.</li> <li>• <b>Remove:</b> Stops the application and removes it from the computer.</li> </ul> <p>The <b>Quarantine</b>, <b>Terminate</b>, and <b>Remove</b> actions apply when the specified application runs. The <b>Ignore</b> and <b>Log only</b> action apply when Symantec Endpoint Protection detects the application.</p>
---	--

## Known Security Risks Exceptions

Use this dialog box to select the known security risks that virus and spyware scans should exclude.

[Security risk ratings](#) describes the information that is provided for each security risk to help you to determine whether or not to make the risk an exception.

If you want to log future detections, you can check the **Log when the security risk is detected** check box.

**Table 270: Security risk ratings**

Field	Description
<b>Security Risk</b>	The name of the security risk. Click the name to display a Symantec web page that provides more information about the risk.
<b>Risk Category</b>	The type of security risk, such as Adware, Misleading Application, or Spyware. The category types change over time as Symantec gets new information about risks.
<b>Overall Rating</b>	The general assessment of the severity of the security risk. This assessment is based on the combination of the security risk's privacy, performance, stealth, and removal ratings.
<b>Privacy Impact</b>	The degree to which the security risk threatens your private information.
<b>Performance</b>	The degree to which the security risk affects your computer's performance.
<b>Stealth Rating</b>	The degree to which the security risk tries to hide to prevent detection and removal.
<b>Removal Rating</b>	The degree to which the security risk makes itself easy to remove.
<b>Dependent Program</b>	The specification of whether a program relies on the security risk to function properly or not.

## Folder Exception

Use this dialog box to exclude a folder from detection on the computers that run Windows. You can choose whether the exception applies to security risk scans, SONAR, or application control.

**Table 271: Folder options**

Option	Description
<b>Prefix variable</b>	<p>A prefix variable indicates a well-known Windows folder. Select a prefix variable to apply the exception on the client computers that run different Windows operating systems. If you select a prefix variable, the path name should be relative to the selected prefix variable.</p> <p><b>Note:</b> The prefix variable applies to 32-bit and 64-bit folders. For example, if you select <b>[PROGRAM_FILES]</b>, both the Program Files (x86) and the Program Files folders are excluded.</p> <p><a href="#">File and Folder Prefix Variables</a></p>
<b>Folder</b>	Type the full path name if the selected prefix variable is <b>[NONE]</b> . If you selected a prefix variable, the path should be relative to the selected prefix.
<b>Include subfolders</b>	Check to include all the subdirectories of the specified folder.
<b>Specify the type of scan that excludes this folder</b>	<p>You can specify whether security risk scans, SONAR, application control, or any combination of the three exclude the folder from detection. You must select at least one type.</p> <p>When you select <b>Security Risk</b>, the <b>Specify the type of security risk scan</b> option appears. You can configure a security risk folder exception to apply only to Auto-Protect scans, scheduled and on-demand scans, or all security risk scans.</p> <p>If you run an application that writes many temp files to a folder, you might want to exclude the folder from Auto-Protect. Auto-Protect scans files as they are written so you can increase computer performance by limiting the exception to scheduled and on-demand scans.</p> <p>You might want to exclude the folders that are not often used or that contain archived or packed files from scheduled and on-demand scans. For example, scheduled or on-demand scans of deeply archived files that are not often used might decrease computer performance. Auto-Protect still protects the folder by scanning only when any files are accessed or written to the folder.</p>

## File Access Exception

Use this dialog box to block malicious files on the client. You use a file access exception to block files that are not executables, such as PDF files, Word documents, and scripts (PowerShell, JavaScript, and VBScript). The client uses the file's hash value to detect and then block the application from accessing the file.

Option	Description
<b>Specify the action to take on this file</b>	<ul style="list-style-type: none"> <li>• <b>Quarantine:</b> Blocks the file from opening and quarantines it on the client computer.</li> <li>• <b>Block:</b> Blocks the file from opening on the client computer.</li> <li>• <b>Log only:</b> Allows the file to open on the client computer and adds an event in the Application Control log.</li> <li>• <b>Ignore:</b> Allows the file to open on the client computer.</li> </ul>
<b>File Fingerprint</b>	The hash value for the file. This field is required. Use either the SHA-256 or a MD5 hash.

Option	Description
<b>Specify at least one of the following attributes for the file or the application that accesses the file</b>	<p>You must specify at least one other attribute for the client to detect the file. These fields are optional.</p> <ul style="list-style-type: none"> <li>• <b>File size:</b> Symantec recommends that you add the file size to improve client performance. Include the file size by bytes, such as 372 KB.</li> <li>• <b>File path:</b> The file's path, name, and extension, such as <code>c:\Users\richard_smith\Documents\TaxDocuments.doc</code>. You can use the wildcards * or ? if you do not know the full path or if you want to include multiple files. For example: <code>c:\Users\richard_smith\*.doc</code>. If you do not know whether the file type is an executable or not, use the quarantine action. The quarantine action ensures that if the file is an executable, it cannot be launched.</li> <li>• <b>Application that accesses the file:</b> Add information about the type of application. For example, a malicious file may use a misleading file extension, such as a PDF file when the file is really a DOC file. If you do not enter any values in the text field, the client blocks any application that might access the file. <ul style="list-style-type: none"> <li>– <b>Application path:</b> For example: <code>C:\Program Files (x86)\Microsoft Office\Office16\Winword.exe</code>. You can use the wildcards * or ?.</li> <li>– <b>Application fingerprint:</b> The application's hash value. Use either the SHA-256 or a MD5 hash.</li> </ul> </li> </ul>

## File Exception

Use this dialog box to exclude a file from detection on the computers that run Windows. You can choose whether the exception applies to security risk scans, SONAR, or application control.

**Table 272: File options**

Option	Description
<b>Prefix variable</b>	<p>A prefix variable indicates a well-known Windows folder. Select a prefix variable to apply the exception on the client computers that run different Windows operating systems. If you select a prefix variable, the file name should be relative to the selected prefix variable.</p> <p>Select <b>[NONE]</b> if you want to use the exception on a specific operating system.</p> <p><b>Note:</b> The prefix variable applies to 32-bit and 64-bit folders. For example, if you select <b>[PROGRAM_FILES]</b>, both the Program Files (x86) and the Program Files folders are excluded.</p> <p><a href="#">File and Folder Prefix Variables</a></p>
<b>File (include full path)</b>	Type the full path name if the selected prefix variable is <b>[NONE]</b> . If you selected a prefix variable, the path should be relative to the selected prefix.
<b>Specify the types of scans that will exclude this file</b>	<p>You can specify whether security risk scans, SONAR, application control, or any combination of the three exclude the file from detection. You must select at least one type.</p> <p>For an application control scan, you can exclude child processes when you exclude a file.</p>
<b>Specify the type of security risk scan</b>	<p>You can configure a security risk file exception to apply only to Auto-Protect scans, scheduled and on-demand scans, or all security risk scans.</p> <p>This option only appears when <b>Security Risk</b> is selected for <b>Specify the types of scans that will exclude this file</b>.</p>

## File and Folder Prefix Variables

When you use all prefix variables (except SYSTEM\_DRIVE), you must include the leading '\' in your path.



---

**NOTE**

You cannot use wildcards.

**Table 273: File and folder options**

Variable	Description
<b>COMMON_APPDATA</b>	The file system folder containing application data for all users: <ul style="list-style-type: none"><li>• C:\Documents and Settings\All Users\Application Data (Windows XP)</li><li>• C:\ProgramData (Windows Vista+)</li></ul>
<b>COMMON_DESKTOPDIRECTORY</b>	The file system folder that contains files and folders that appear on the desktop for all users: <ul style="list-style-type: none"><li>• C:\Documents and Settings\All Users\Desktop (Windows XP)</li><li>• C:\Users\Public\Desktop (Windows Vista+)</li></ul>
<b>COMMON_DOCUMENTS</b>	The file system folder that contains documents that are common to all users: <ul style="list-style-type: none"><li>• C:\Documents and Settings\All Users\Documents (Windows XP)</li><li>• C:\Users\Public\Documents (Windows Vista+)</li></ul>
<b>COMMON_PROGRAMS</b>	The file system folder that contains the folders for the common program groups that appear on the Start menu for users: <ul style="list-style-type: none"><li>• C:\Documents and Settings\All Users\Start Menu\Programs (Windows XP)</li><li>• C:\ProgramData\Microsoft\Windows\Start Menu\Programs</li></ul>
<b>COMMON_STARTUP</b>	The file system folder that contains all the programs that appear in the Startup folder for all users: <ul style="list-style-type: none"><li>• C:\Documents and Settings\All Users\Start Menu\Programs\Startup (Windows XP)</li><li>• C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup (Windows Vista+)</li></ul>
<b>PROGRAM_FILES</b>	The Program Files folder, which includes: <ul style="list-style-type: none"><li>• C:\Program Files</li><li>• C:\Program Files (x86)</li></ul>
<b>PROGRAM_FILES_COMMON</b>	The folders for components that are shared across applications: <ul style="list-style-type: none"><li>• C:\Program Files\Common Files</li><li>• C:\Program Files (x86)\Common Files</li></ul>
<b>SYSTEM</b>	The Windows System folder: <ul style="list-style-type: none"><li>• C:\Windows\System32</li></ul>
<b>SYSTEM_DRIVE</b>	Indicates the location where the Windows operating system is installed (new in 14.0): <ul style="list-style-type: none"><li>• C:\</li></ul>
<b>USER_PROFILE</b>	File system folders that correspond to all the users (new in 14.0): <ul style="list-style-type: none"><li>• C:\Users\%user% (Windows Vista+)</li></ul>
<b>WINDOWS</b>	The Windows folder or SYSROOT, which corresponds to the %windir% or %SYSTEMROOT% environmental variables: <ul style="list-style-type: none"><li>• C:\Windows</li></ul>

## Security Risk Extension Exceptions

Type the name of the extension that you want to exclude from future virus and spyware scans in the text box. You can add only one extension at a time. You can include a space in an extension name. You can select whether the exception applies to all types of security risk scans, or a particular type of security risk scan.

If you want to add multiple extensions, type a single extension name and then add the extension. Repeat this step for each extension that you want to add.

### NOTE

If you enter multiple extension names in the **Add** text box, the policy treats the entry as a single extension name.

## Security Risk File or Folder Exception for Mac clients

You can specify an exception for files or folders on Mac clients.

### WARNING

You must also specify the setting to enable exceptions in the Auto-Protect settings for Mac clients.

[Mac Auto-Protect: Scan Details](#)

### NOTE

Folder paths for Mac clients must be denoted by using a forward slash. A backward slash is used for Windows paths.

**Table 274: File or folder exceptions for Mac clients**

Option	Description
<b>Prefix variable</b>	<p>You can specify a common top-level location on the client.</p> <p>You can choose from the following prefix variables:</p> <ul style="list-style-type: none"><li>• <b>HOME</b> The home folder for the user that is currently logged on. A home folder path is typically /Users/username, where username matches the user name of the logged on user.</li><li>• <b>APPLICATION</b> The system application folder, which is /Applications.</li><li>• <b>LIBRARY</b> The folder for common system libraries, which is /Library.</li></ul> <p>The default is <b>NONE</b>.</p>
<b>File or folder</b>	<p>You can specify files or folders relative to the prefix variable. If you did not choose a prefix variable, then enter the full file path.</p> <p>The use of symbolic links (symlinks) in this field is not supported. For example, /var is a symbolic link representing /private/var. If you define a path with /var, the scan does not work as expected. You must define the file path with /private/var/.</p>

## Trusted Web Domain Exception

You can exclude a web domain from Download Insight detections and SONAR. When you exclude a web domain, files that users download from any location in that web domain are always allowed. Any allowed files, however, are scanned by Auto-Protect and any administrator- or user-defined scans.

Trusted Web Domain exceptions require Download Insight.

---

## NOTE

By default, Download Insight does not examine any files that users download from a trusted Internet or intranet site. You configure trusted sites and trusted local intranet sites on the **Windows Control Panel > Internet Options > Security** tab. You can disable the Download Insight setting for intranet sites in the Virus and Spyware Protection policy.

## NOTE

The Trusted Web Domain exceptions work with URL reputation in the Intrusion Prevention policy. The URL reputation allows any web domain that you add as an exception. URL reputation allows or blocks access to the web addresses that are identified as known sources of the malicious content.

You must enter a single domain or IP address when you specify a trusted Web domain exception. You can specify only one domain at a time. Port numbers are not supported. You must specify an IP address for an FTP location.

You can specify a URL, but the exception uses only the domain name portion of a URL. If you specify a URL, you can prepend the URL with either HTTP or HTTPS (case-insensitive), but the exception applies to both.

**For example, any one of the following entries produces the same exception:**

- `test.domain.com`
- `test.domain.com/mydocs`
- `HTTP://test.domain.com/mydocs`
- `https://test.domain.com`

Regardless of whether a user navigates to `test.domain` through HTTP or HTTPS, Download Insight and SONAR exclude the domain. If the user navigates to any location within the domain (such as `mydocs`), the user can download files from that location.

When you specify an IP address, the exception applies to both the specified IP address and its corresponding host name.

For FTP locations, for example, you must specify an IP address. If a user navigates to the FTP location through its URL, Symantec Endpoint Protection resolves the host name to the IP address and applies the exception.

The following table displays examples of domain name matching logic:

URL	If user accesses	Client Allows or blocks the website
fakebook.com		Allowed
	www.fakebook.com	Blocked (due to exact match)
www.fakebook.com	fakebook.com	Blocked (due to exact match)
	www.fakebook.com	Allowed
*fakebook.com	fakebook.com	Blocked (* must match something)
	www.fakebook.com	Allowed (* matches "www")
pastebin.com	pastebin.com/eSsjmhBG	Still blocked (Doesn't impact Scanner feature)
*.wicar.org	http://malware.wicar.org/data/java_jre17_exec.html	The client does not receive an SID:60501 event as the WebFilter allows this URL; but the scanner still blocks the URL.

View the Download Risk Distribution report to find the URLs and IP addresses for the Web domains that you want to exclude.

## Tamper Protection Exception

Use this dialog box to exclude a file from detection by Tamper Protection.

---

## NOTE

Tamper Protection does not support folder exceptions.

**Table 275: Tamper Protection exception options**

Option	Description
<b>Prefix variable</b>	<p>A prefix variable indicates a well-known Windows folder. Select a prefix variable to apply the exception on the client computers that run different Windows operating systems. If you select a prefix variable, the file name should be relative to the selected prefix variable.</p> <p>Select <b>[NONE]</b> if you want to use the exception on a specific operating system.</p> <p>The default is <b>[NONE]</b>.</p> <p><b>Note:</b> The prefix variable applies to 32-bit and 64-bit folders. For example, if you select <b>[PROGRAM_FILES]</b>, both the Program Files (x86) and the Program Files folders are excluded.</p>
<b>File (include full path)</b>	<p>Type the full path name if the selected prefix variable is <b>[NONE]</b>. If you selected a prefix variable, the path should be relative to the selected prefix.</p> <p>You must specify a file name. Tamper Protection does not support folder exceptions. If you enter a folder name, Tamper Protection does not exclude all the files in a folder with that name. It only excludes a file with that specified name.</p>

### [File and Folder Prefix Variables](#)

## DNS or Host File Change Exception

Use this dialog box to create a hash-based exception for an application that makes a DNS or host file change. SONAR might prevent system changes like DNS or host file changes. You might need to make an exception for a VPN application, for example.

You can monitor the VPN application so that it appears in this dialog as a monitored application. Use this dialog to specify how Symantec Endpoint Protection handles the application when it tries to modify DNS settings or change a host file.

## NOTE

The DNS or host file change exception does not exempt the application from detection by SONAR. SONAR always detects the application if it exhibits suspicious behavior.

**Table 276: DNS or host file change exception**

Option	Description
<b>View</b>	<p>You can filter the applications by the following types:</p> <ul style="list-style-type: none"><li>• <b>All</b> Shows all detected applications.</li><li>• <b>Watched Applications</b> The applications that you specified as Application to Monitor exceptions.</li><li>• <b>User-allowed Applications</b> User-allowed applications are the applications that users choose to allow when they try to download files.</li></ul> <p><b>Note:</b> If you change an application's file name and configure an exception to monitor that application with its new file name, the application does not appear in the watched applications list with its new name. Instead the application appears in the unfiltered list with its original name.</p>
<b>Action</b>	<p><b>You can specify any of the following actions:</b></p> <ul style="list-style-type: none"><li>• <b>Ignore</b> Excludes the application from detection when it makes a DNS or host file change.</li><li>• <b>Log only</b> Adds an entry in the SONAR log when SONAR detects a DNS or host file change that is made by the specified application.</li><li>• <b>Prompt</b> Prompts the user to allow or block a DNS or host file change by the specified application.</li><li>• <b>Block</b> Stops the application from making a DNS or host file change.</li></ul> <p><b>Note:</b> SONAR applies the specified action when the application tries to make a host file change or modify DNS settings. SONAR does not apply an action when the application only opens or accesses a host file or a file that contains DNS settings.</p>

## Add Folder Exception for Linux clients

Use this dialog box to exclude a folder from detection on the client computers that run Linux. You can choose whether the exception applies to all scans, only to Auto-Protect scans, or only to scheduled and on-demand scans.

**Table 277: Folder exception options for Linux clients**

Option	Description
<b>Prefix variable</b>	<p>A prefix variable indicates a well-known Linux folder. Select a prefix variable to apply the exception on the client computers that run different Linux distributions.</p> <ul style="list-style-type: none"> <li>• <b>ROOT</b> The path to the home directory of the root user, also called superuser. Typically, this directory is /root.</li> <li>• <b>HOME</b> The path to the user home directories. Typically, this directory is /home.</li> <li>• <b>BIN</b> The path to the directory that contains user commands. Typically, this directory is /bin.</li> <li>• <b>ETC</b> The path to the directory that contains configuration files and directories. Typically, this directory is /etc.</li> <li>• <b>USR</b> The path to the directory that contains user-related files and directories, such as programs and supporting library files. Typically, this directory is /usr.</li> <li>• <b>OPT</b> The path to the directory that contains optional files and programs. Typically, this directory is /opt.</li> </ul> <p>The default is <b>NONE</b>.</p>
<b>Folder</b>	Enter the full path name if the selected prefix variable is <b>NONE</b> . If you selected a prefix variable, the path should be relative to the selected prefix.
<b>Also exclude subfolders</b>	<p>Check to include all the subdirectories of the specified folder.</p> <p>As of 14.3 RU1, this option is not supported in Symantec Agent for Linux and all subdirectories are always excluded from the scans.</p>
<b>Specify the type of security risk scan</b>	<p>You can specify a security risk folder exception to apply only to Auto-Protect scans, only to scheduled and on-demand scans, or to all security risk scans.</p> <p>If you run an application that writes many temp files to a folder, you might want to exclude the folder from Auto-Protect. Auto-Protect scans files as they are written so you can increase computer performance by limiting the exception to scheduled and on-demand scans.</p> <p>You might want to exclude the folders that are not often used or that contain archived or packed files from scheduled and on-demand scans. For example, scheduled or on-demand scans of deeply archived files that are not often used might decrease computer performance. Auto-Protect still protects the folder by scanning only when any files are accessed or written to the folder.</p>

## Add Certificate Exception

Use this dialog box to exclude a certificate to keep the files that it signs from being flagged as suspicious. You browse to the certificate to add an exclusion for it. Once you add the certificate, information about the certificate's signer and issuer appears along with the SHA-1 thumbprint. The certificate does not have to be installed on the client computer for the exclusion to work.

You can only add a certificate exception in Symantec Endpoint Protection Manager if it is unenrolled from the cloud console. If Symantec Endpoint Protection Manager is enrolled, use the cloud console to add or manage a certificate exception.

The default action for this exception is **Ignore**.

**Table 278: Certificate exception options**

Option	Description
<b>Certificate File</b>	<p>Next to <b>File location</b>, click <b>Browse</b> to navigate to the certificate.</p> <p>Supported certificate types:</p> <ul style="list-style-type: none"><li>• DER</li><li>• BASE 64</li></ul> <p>You cannot add a file that is not a certificate. You also cannot add a duplicate of a certificate for which you have already added an exception.</p>
<b>Certificate Information</b>	<p>Once you add the certificate, the following information is displayed about it:</p> <ul style="list-style-type: none"><li>• Issuer The certificate authority that issued the certificate.</li><li>• Signer The entity that signed the certificate.</li><li>• SHA-1 thumbprint The certificate's SHA-1 hash value. This value defines the exception and determines whether the certificate you add is a duplicate of a certificate you already added.</li></ul> <p>These values are read directly from the certificate and are read-only. You cannot manually input the values into these fields, nor can you edit them.</p>

[Excluding a certificate from scans on Windows clients](#)

## LiveUpdate Settings Policy

### LiveUpdate Server Settings for Windows clients

You use this page to specify how Windows clients get updates to virus and spyware definitions, intrusion prevention signatures, and other protection technologies.

**Table 279: LiveUpdate Server Settings for Windows clients**

Setting	Description
Internal or External LiveUpdate Server	<p><b>Both options are enabled by default.</b></p> <ul style="list-style-type: none"> <li>• <b>Use the default management server</b> Downloads the content updates from the Symantec Endpoint Protection Manager. This option is recommended for most organizations. The option is the simplest and requires no configuration other than applying the policy to a group. Select this option if you use a Group Update Provider.</li> <li>• <b>Use a LiveUpdate server</b> Downloads the content updates from one of the following options: <ul style="list-style-type: none"> <li>– The default Symantec LiveUpdate server over the Internet</li> <li>– An internal LiveUpdate server You can specify multiple internal LiveUpdate servers for failover support.</li> <li>– The Symantec Early Adopter server The Symantec Early Adopter server lets you test upcoming engine updates before they are released. If you select this server, <b>Use the default management server</b> is unchecked and disabled.</li> </ul> </li> </ul> <p>When both options are enabled, and if all other LiveUpdate policy settings use the default values, clients always prefer the Symantec Endpoint Protection Manager. In the default scenario, the client gets updates from a LiveUpdate server only in the following cases:</p> <ul style="list-style-type: none"> <li>• If you let the client initiate a LiveUpdate session</li> <li>• (Default) When the client requests full definitions from the management server, but can get a smaller package from a LiveUpdate server</li> <li>• If the client is significantly out-of-date and cannot connect to the management server</li> </ul> <p><a href="#">LiveUpdate Settings Policy: Windows Schedule</a></p>
Group Update Provider	<p><b>Use a Group Update Provider</b></p> <p>Specifies one or more computers to act as a LiveUpdate server for the group. For example, you might want to create a Group Update Provider to conserve bandwidth to clients in a remote location over a slow link. In this scenario, the Group Update Provider downloads the latest updates from the server. The Group Update Provider then updates the clients in the group. If the Group Update Provider is offline, the clients contact the server for the updates. A Group Update Provider can reside in any group.</p> <p><b>Note:</b> Group Update Providers are available only for Windows clients.</p>
Third Party Management	<p><b>Enable third-party content management</b></p> <p>Enables third-party tools such as Microsoft SMS to provide updates to client computers securely. To use this feature, you must set up the Symantec Endpoint Protection Manager as a staging server for content. This staging server does not require that the clients be connected to it. Configure the server to download updates on a periodic schedule. If you specify the <b>Continuously</b> scheduling option, the server downloads the latest updates as soon as they are posted.</p> <p><a href="#">Download Schedule</a></p> <p>By default, the updates appear in the Default group's clients' content outbox folders. These folders are organized by content type. You can then pick up one or more content packages from the content outbox folder and deliver it to the client's inbox folder.</p> <p>To ensure that only third-party management tools update client computers, disable the other LiveUpdate server options on this page.</p> <p><b>Note:</b> Third-party content management settings are applied to Windows clients only.</p> <p><a href="#">Using third-party distribution tools to update client computers</a></p>



Setting	Description
<b>LiveUpdate Proxy Configuration</b>	Configure a proxy server to use for LiveUpdate from the default Symantec LiveUpdate server or from a specified internal LiveUpdate server. This proxy server is used only for LiveUpdate and not for any other external communications.

## LiveUpdate Settings Policy: Windows Schedule

Lets you specify how often to push updates from LiveUpdate servers to Windows clients in the groups to which this policy is applied. These settings are applied only if you enable a LiveUpdate server at **LiveUpdate Policy > Windows Settings > Server Settings**.

[LiveUpdate Server Settings for Windows clients](#)

**Table 280: LiveUpdate schedule settings for Windows clients**

Option	Description
<b>Enable LiveUpdate Scheduling</b>	Lets your Windows clients run scheduled LiveUpdate sessions. You then set the scheduling options that the clients use when they communicate with any LiveUpdate server. This option is enabled by default.
<b>Frequency</b>	Specifies how often clients run LiveUpdate to download the latest updates. The default is <b>Every</b> 4 hours. The specific time option is available for both <b>Daily</b> and <b>Weekly</b> options. The specific day option is available for the <b>Weekly</b> setting only. The <b>Continuously</b> option allows the client computers that infrequently communicate with the Symantec Endpoint Protection Manager to get the latest updates. They get the latest updates when they connect to the network and authenticate to the server.
<b>Retry Window</b>	Specifies the number of hours or days to keep trying to run LiveUpdate if the scheduled session failed. This option is enabled if the Every, Daily or Weekly option is selected.
<b>Download Randomization Options</b>	Specifies a randomization option. You can stagger the updates, plus or minus the value that is specified, to minimize the effect on network traffic. By default, Symantec Endpoint Protection randomizes the LiveUpdate sessions to minimize bandwidth spikes.
<b>Idle Detection</b>	Specifies that a scheduled LiveUpdate should not run until the client computer is idle. If the computer is never idle, then after the final threshold is reached, LiveUpdate runs even if the computer is not idle. If unchecked, the scheduled LiveUpdate always runs at the scheduled time, regardless of how busy the computer is.
<b>Options for Skipping LiveUpdate</b>	Specifies that LiveUpdate should run at the next scheduled time only if the checked criteria are met. If the client does not meet either criterion, then the scheduled LiveUpdate is skipped and an entry is made in the client system log.

[Configuring the LiveUpdate download schedule to client computers](#)

## LiveUpdate Settings Policy - Advanced Settings

Table 281: LiveUpdate Settings policy

Setting	Description
<b>User Settings</b>	<p>These settings are available for end users on Windows computers. LiveUpdate can always be launched manually on a client computer that runs Mac.</p> <ul style="list-style-type: none"> <li>• <b>Allow the user to manually launch LiveUpdate</b> Lets the users manually perform LiveUpdate on client computers. Disable this setting as a best practice for managed clients. Conflicts can occur if a scheduled LiveUpdate session is running when a user manually starts a LiveUpdate session.</li> <li>• <b>Allow the user to modify the LiveUpdate schedule</b> Lets the users change LiveUpdate schedule settings on client computers. If an unmanaged client has a LiveUpdate Settings policy that is part of an install package, the policy settings take precedence over a user's changes. To install an unmanaged client that retains a user's changes to LiveUpdate settings, install the client from the installation file. Do not use a client install package that you exported from the Symantec Endpoint Protection Manager.</li> <li>• <b>Allow the user to modify HTTP, HTTPS, or FTP proxy settings for LiveUpdate</b> Lets the users change LiveUpdate proxy settings on client computers.</li> </ul>
<b>Download client patches</b>	<p>Downloads and installs client patches to fix security vulnerabilities and critical fixes in the Windows client in between releases. Client patches are included in a delta file, and then downloaded to the client as with other content types. These patches do not include major features. You can download the content to the clients using a LiveUpdate server, the management server, or a Group Update Provider. The method you use depends on how you configured server settings in the LiveUpdate Settings policy. Disabled by default.</p> <p>The client must be the same version as the management server for the client patches to install. If the client and the management server are different versions, then use AutoUpgrade to upgrade the clients to be the same version as the management server.</p> <p>You should also verify that the LiveUpdate server downloads client patches to Symantec Endpoint Protection Manager for the site.</p> <p>This option was renamed from <b>Download client security patches</b> in 14.3 RU2.</p> <p><a href="#">Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager</a></p> <p><a href="#">Installing Endpoint Protection client patches on Windows clients</a></p> <p><a href="#">Choose a distribution method to update content on clients</a></p>
<b>Product Update Settings</b>	<p>Downloads and installs client software updates automatically when users click LiveUpdate or when a scheduled LiveUpdate session runs. If this setting is turned off, the client cannot download and install product updates, even if another Symantec product runs LiveUpdate on the client computer.</p> <p>If the LiveUpdate Settings policy specifies that clients download updates from a Symantec Endpoint Protection Manager or Group Update Provider, the updates are in the form of microdefs. If the LiveUpdate Settings policy specifies that clients download updates from a LiveUpdate server, the updates are in the form of MSP (patch) files.</p> <p>This setting lets you control client software versions. When this setting is disabled, client software can only be manually updated. When the management server downloads and processes patches, it creates a microdef. Microdefs automatically appears as new packages. The new package appears in the Client Install Packages pane. You can then select the package, and use the Upgrade feature for your Windows clients. You must provide manual updates for Mac clients by using a third-party tool or by making the update package available for download on your network.</p> <p>If you want to keep strict control of the client software revisions that your clients use, do not enable them to download product updates.</p>

Setting	Description
<b>Download delta content from a LiveUpdate server when available</b> (14.3 RU2 and later)	<p>If the management server can provide only a full set of content (such as virus and spyware definitions or client patches) to your clients, you can let these clients get smaller packages (deltas) from a LiveUpdate server. This situation can occur when the management server cannot provide the appropriate deltas to the clients. Too many simultaneous client requests for full definitions can create an excessive load on your network. This setting helps reduce the risk of such a load.</p> <p>The management server can fail to store a delta for various reasons, such as a network outage or a server backup to an older definitions set.</p> <p>You may also want to check the number of content revisions that the management server stores. If this number is low, very out-of-date clients may not be able to get deltas from the management server.</p> <p>This option was renamed from <b>Download smaller client installation packages from a LiveUpdate server when available</b> in 14.3 RU2.</p> <p><a href="#">Mitigating network overloads for client update requests</a></p>

## Group Update Provider

The Group Update Provider (GUP) gets content updates from the Symantec Endpoint Protection Manager and locally distributes the updates to groups of clients. For each LiveUpdate Settings policy, you can configure any one of the following types of Group Update Providers.

**Table 282: Group Update Provider selection options for clients**

Setting	Description
<b>Multiple Group Update Providers</b>	<p>Use this option when you have multiple groups and want to use different Group Update Providers for each group.</p> <p>Multiple Group Update Providers use a set of rules, or criteria, to elect themselves to serve groups of clients in their own subnets. All client computers are on the same subnet.</p>
<b>Explicit Group Update Providers for roaming clients</b>	<p>Use this option when you want clients to be able to connect to Group Update Providers that are on subnets other than the client's subnet. Clients that change location can roam to the closest Group Update Provider on the list.</p> <p>If you add an explicit list, you do not create actual Group Update Providers. You must also specify the Group Update Providers themselves in another LiveUpdate Settings policy.</p> <p><a href="#">Configure Explicit Group Update Providers</a></p>
<b>Single Group Update Provider IP address or host name</b>	<p>Use a single Group Update Provider so that a single client computer acts as the same Group Update Provider for all your clients in a group.</p> <p>Type the IP address or host name of the client computer.</p> <ul style="list-style-type: none"> <li>• Example IPv4 address: 192.168.0.10</li> <li>• Example IPv6 address: 2001:DB8:3C0:FC01:49C8:C72A::10</li> <li>• Example host name: gupServer1</li> </ul> <p>Depending on your network setup, you may need to use the full DNS name as the host name. You can use the wild-card asterisk (*) and question mark (?) characters in the host name.</p>
<b>Maximum time that clients try to download updates from a Group Update Provider before trying the default management server</b>	<p>This option lets clients bypass a Group Update Provider if they try and fail to connect to the Group Update Provider. You can specify a length of time after which clients can bypass the Group Update Provider. When clients bypass the Group Update Provider, they get content updates from the default server.</p> <ul style="list-style-type: none"> <li>• Check <b>Never</b> if clients only get updates from the Group Update Provider and never from the server. For example, you might use this option if you do not want client traffic to run over a wide area connection to the server.</li> <li>• Check <b>After</b> to specify the time after which clients must bypass the Group Update Provider. If you set this time to 15 minutes, this means that the client computer must try to download continuously for 15 minutes with no success.</li> </ul>

The Group Update Provider does not act as a proxy for operational states, events, commands, command status, or profiles between the server and the clients.

**Table 283: Group Update Provider settings**

Setting	Description
<b>Default port</b>	<p>The TCP port that is used for client communications.</p> <p>The default TCP port number is 2967. If the GUP receives IP addresses with DHCP, you should assign a static IP address to the computer or use the host name. If the GUP is at a remote location that uses network address translation (NAT), use the host name.</p> <p><b>Note:</b> If the GUP runs a non-Symantec firewall, you might need to modify the Symantec Firewall policy to permit the TCP port to receive server communications. A non-Symantec firewall refers to Windows firewall and third-party firewalls. By default, the Symantec Firewall policy is configured automatically.</p>
<b>Maximum disk cache size allowed for downloading updates (MB)</b>	<p>The maximum disk space that the GUP can use to store content updates. When this limit is reached, the GUP no longer downloads content from the management server. However, it does continue to serve the content in the cache to its clients.</p>
<b>Delete content updates if unused (days)</b>	<p>The content updates take up disk space on the Group Update Provider computer. Configure this option to delete unused content updates. Content updates are considered unused if the clients have not requested the updates.</p>
<b>Maximum number of simultaneous downloads to clients</b>	<p>Conserves the memory and CPU utilization on the GUP computer. The option controls how many threads are allocated to handle incoming requests. More threads require more memory. Also, processing the incoming requests requires CPU cycles, so more threads require more CPU cycles.</p> <p>You should tune the value to the limitations of the GUP computer. The goal is to download content updates to clients as quickly as possible, without overwhelming the Group Update Provider computer. Set the value high enough to get reasonable concurrency, but low enough to avoid overwhelming the Group Update Provider computer.</p>
<b>Maximum bandwidth allowed for Group Update Provider downloads from the management server</b>	<p>Controls the amount of bandwidth that the GUP uses to download content updates from the management server. Symantec recommends that you explicitly limit bandwidth according to the limitations of the GUP computers.</p> <p><b>Select one of the following options:</b></p> <ul style="list-style-type: none"><li>• Check <b>Unlimited</b> to allow effectively unlimited bandwidth. This option enforces an actual limit of 1 MB. Under normal circumstances, however, this limit is never reached.</li><li>• Check <b>Up to</b> to limit the bandwidth to the amount that you specify. This option lets you specify bandwidth above and below the 1 MB limit that the <b>Unlimited</b> option enforces.</li></ul>
<b>Maximum bandwidth allowed for client downloads from Group Update Provider</b>	<p>Controls the amount of bandwidth between the GUP computer and the clients that the GUP services.</p> <p>Use this option if you can set up only one GUP for multiple sites, and each site has a few clients only or has low connectivity. Minimize the bandwidth for the sites that have low connectivity or where you want to avoid content storms because the GUP delivers a full set of content definitions. Use the <b>Unlimited</b> option if clients with low-bandwidth connections receive the full definitions file. The GUP has limited threads to serve download requests. Clients that receive a full definitions file take a long time and reduce the GUP's thread by one until the definitions are downloaded.</p>

## Configuring clients to download content from Group Update Providers

### Group Update Provider List

You use this dialog box to add the rules that a client must match to act as a Group Update Provider.

**Rules are structured as follows:**

---

- Rule sets

Each rule set is a container to hold the rules. The rule set appears as a tree node.

Rule sets are matched based on the logical OR and AND operators. If multiple rule sets are OR'ed, a client must match at least one rule set to act as a Group Update Provider. If multiple rule sets are AND'ed, a client must match every rule that is specified in a rule set to act as a Group Update Provider.

- Rule types

Rules specify IP addresses, host names, Windows client registry keys, or client operating systems. You can include one of each rule type in a rule set.

- Rule conditions

A rule specifies a condition that a client must match to act as a Group Update Provider. Multiple values for a rule condition are OR'ed. If a rule specifies a condition with multiple values, the client must match one of the values.

For example, you might create RuleSet1 that includes a rule with several IP addresses. You then create RuleSet2 that includes a host name rule and an operating system rule, each with multiple values. A client computer must match either RuleSet1 or RuleSet2. A client matches RuleSet1 if it has any one of the IP addresses. A client matches RuleSet2 only if it has one of the host names and if it runs one of the specified operating systems.

## Specify Group Update Provider Rule Criteria

You use this dialog box to add a rule that a client must match to act as a Group Update Provider. The rule types include an IP address or host name, registry keys, and operating system.

You can specify one rule of each type, with multiple criteria for each rule. Rules are matched based on the logical OR and AND operators. Multiple rules are AND'ed; a client must match all the rules in one rule set. Multiple rule criteria are OR'ed; a client must match one criterion in each rule.

For the host name, you may need to use the full DNS name, depending on your network setup.

## Configure Explicit Group Update Providers

Use this dialog box to add a list of Group Update Providers that the clients can connect to that are on subnets other than the client's own subnet. Clients that change location frequently can roam to the closest Group Update Provider on the list.

Configuring single or multiple Group Update Providers turns clients into Group Update Providers. Configuring an Explicit Group Update Provider list does not turn clients into Group Update Providers. Therefore, you can use an explicit list only as long as you have configured single or multiple Group Update Providers in at least one other policy in the Symantec Endpoint Protection Manager.

Clients try to connect to Group Update Providers in the order that is specified in the list. If the entry is of type subnet, it expands to include all of the available Group Update Providers in the subnet. Clients try to connect to Group Update Providers in the subnet in the ascending order of their IP addresses.

Explicit Group Update Providers can be static or dynamic, depending on how you configure them. If you use an IP address or a host name to configure an explicit Group Update Provider, then it is a static Group Update Provider. This difference affects how Group Update Providers act in those networks that mix clients and management servers from the current release and an earlier release.

If you use a subnet to designate a Group Update Provider, it is dynamic, as clients search for a Group Update Provider on that subnet.

## Add Explicit Group Update Provider

Adding an explicit Group Update Provider does not turn a client into a Group Update Provider. Adding explicit Group Update Providers maps the clients' subnets to one or more subnets where Group Update Providers are located.

You use an explicit Group Update Provider list to map the client subnet network addresses to the Group Update Providers. You identify the Group Update Providers by using their IP address, host name, or subnet.

You can specify that the clients with IP addresses that fall on a particular subnet should use a particular Group Update Provider.

A client may have multiple IP addresses. Symantec Endpoint Protection considers all IP addresses when it matches to a Group Update Provider. The IP address that the policy matches to is not necessarily bound to the interface that the client uses to communicate with the Group Update Provider.

For example, suppose that a Symantec Endpoint Protection client has the following IPv4 addresses:

- 172.21.80.180: Used to communicate with the Symantec Endpoint Protection Manager
- 172.21.66.209: The subnet network address that is mapped in the **Explicit Group Update Providers** list

Or:

- 001:DB8:3C0:FC01:49C8:C72A::10: Used to communicate with the Symantec Endpoint Protection Manager
- 2001:DB8:3C0:FC01::: The subnet network address that is mapped in the **Explicit Group Update Providers** list

The matching address is not necessarily the same address as the interface that the client uses to communicate with the Group Update Provider or with the Symantec Endpoint Protection Manager.

**Table 284: Client subnet network address and explicit Group Update Provider settings**

Option	Description
<b>Client Subnet Network Address</b>	The network address of the clients' subnet. This address is not the IP address of a client itself. If you do not know the clients' subnet network address, you can calculate it by using one of the subnet calculators available on the Internet. This address is sometimes also referred to as the network prefix or network ID.
<b>Specify Client Subnet Mask</b>	Use this setting to add a group of subnets, rather than adding one subnet at a time. For example: <ul style="list-style-type: none"><li>• For IPv4, rather than adding both the 192.168.1.0 subnet and the 192.168.2.0 subnet, you can add the 192.168.0.0 subnet and a mask of 255.255.0.0.</li><li>• For IPv6, rather than adding both the 2001:DB8:3C0:FC01:49C8:1111:: subnet and the 2001:DB8:3C0:FC01:49C8:2222:: subnet, you can add the 2001:DB8:3C0:FC01:49C8:: subnet and a mask of FFFF:FFFF:FFFF:FFFF:FFFF::.</li></ul> If you do not add a client subnet mask, Symantec Endpoint Protection Manager automatically finds the subnet mask based on the clients' NIC settings. Symantec Endpoint Protection Manager then determines the range of IP addresses in the client subnet. If you upgrade from 12.1.6 and earlier, you can add the client subnet mask to existing imported subnets. Otherwise, 12.1.6 and earlier clients ignore this setting.
<b>Type &gt; IP Address</b>	Identifies this Group Update Provider by its IP address. When you select this option, the following other options are displayed: <ul style="list-style-type: none"><li>• <b>IP address</b> The IP address of this Group Update Provider, in IPv4 format.</li><li>• <b>Port</b> The port that this Group Update Provider is on.</li></ul>

Option	Description
<b>Type &gt; Host Name</b>	<p>Identifies this Group Update Provider by its host name. When you select this option, the following other options are displayed:</p> <ul style="list-style-type: none"> <li>• <b>Host Name</b> The host name of this Group Update Provider. The use of wildcard characters is not supported.</li> </ul> <p><b>Note:</b> Depending on your network setup, you may need to use the full DNS name in the Host name field when you configure a Group Update Provider.</p> <ul style="list-style-type: none"> <li>• <b>Port</b> The port that this Group Update Provider is on.</li> </ul>
<b>Type &gt; Subnet</b>	<p>The network address of the subnet on which the Group Update Provider is located. When you select this option, the following other options appear:</p> <ul style="list-style-type: none"> <li>• <b>GUP Subnet Network Address</b> The network address of the subnet that this Group Update Provider is on. Use this type to make multiple Group Update Providers available to match the client network address mapping. If you enter an IP address, Symantec Endpoint Protection Manager automatically finds the subnet mask and determines the range of IP addresses in the Group Update Provider subnet.</li> </ul> <p>You can calculate the value of the <b>GUP Subnet Network Address</b> by using one of the subnet calculators readily available on the Internet. This address is sometimes also referred to as the network prefix or network ID.</p>

## IP Address or Host Name

You use the **IP Address or Host Name** dialog box to specify IP addresses or host names.

**Table 285: IP address or host name rule values**

Setting	Description
<b>Type</b>	You can identify the Group Update Provider by its IP address or by its host name.
<b>IP Address</b>	Type the IP address of the Group Update Provider.
<b>Host Name</b>	<p>Type the host name of the Group Update Provider.</p> <p><b>Note:</b> Depending on your network setup, you may need to use the full DNS name in the Host name field when you configure a Group Update Provider.</p> <p>You can use the wild cards asterisk (*) and question mark (?) in the host name.</p>

## Registry Keys

You use the **Registry Keys** dialog box to specify registry keys.

The Windows registry is a database that stores settings and options for Windows operating systems. The registry contains keys and values. A key is similar to a folder or path. For example, HKEY\_LOCAL\_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\LiveUpdate\Schedule\AllowRetry is a registry key.



**Table 286: Registry key rule values**

Setting	Description
<b>Check</b>	<b>Select one of the following options:</b> <ul style="list-style-type: none"> <li>• <b>Registry Key</b></li> <li>• <b>Registry Key Name</b></li> <li>• <b>Registry Value</b></li> </ul>
<b>Key Name</b>	Type the registry key or registry key name. The Key name is the name of the item in the registry key. An example of a key name is ServiceStatus.
<b>Exists</b> <b>Does not exist</b>	<b>Select one of the following options:</b> <ul style="list-style-type: none"> <li>• Select <b>Exists</b> if the key exists in the Group Update Provider.</li> <li>• Select <b>Does not exist</b> if the key does not exist in the Group Update Provider.</li> </ul>
<b>Equal to</b> <b>Not equal to</b>	<b>Select one of the following options:</b> <ul style="list-style-type: none"> <li>• Select <b>Equal to</b> if the key value equals the specified value.</li> <li>• Select <b>Not equal to</b> if the key value does not equal the specified value.</li> </ul>
<b>Value Type</b>	Select the key data type. <b>The Windows registry uses the following basic data types:</b> <ul style="list-style-type: none"> <li>• <b>String</b> A string comprises plain readable text. String values are the most common values that are used in the registry.</li> <li>• <b>DWORD</b> DWORD stands for double word. DWORD data types comprise binary data that is either limited to 32 bits in length or is entered in decimal or hexadecimal format. <b>Note:</b> If you select the value type DWORD, only decimal format is allowed in the Value field.</li> <li>• <b>Binary</b> Binary is binary data that is displayed in hexadecimal format.</li> </ul>
<b>Value</b>	Type the key value. A value consists of the value of the registry key name, which is stored within the key. The value of the key depends on the value type. A value can also be a name-data pair.

## Operating Systems

Select the operating system.

## Proxy server settings for external communications

- [Proxy server options for Windows](#)  
You can configure Windows a separate proxy server for external communications other than LiveUpdate. Separate settings exist for HTTP proxy configuration and for HTTPS proxy configuration.  
These settings do not affect any other servers or the Group Update Providers that you can configure on the LiveUpdate Settings Policy **Server Settings** tab.
- [Proxy server options for Mac](#)  
For Mac clients, you can configure a proxy server for LiveUpdate communications.



**Table 287: Proxy server options for Windows**

Option	Description
<b>Do not use a proxy server</b>	No proxy server is used.
<b>Use the proxy server specified by the client browser (default)</b>	Use the proxy information that is entered into the browser on the client computers. In Internet Explorer, this information appears in <b>Internet Options &gt; Connections &gt; LAN Settings</b> .
<b>Use custom proxy settings</b>	Use the proxy server information address and the listening port that you enter here. Enter the HTTPS or HTTP port to use.
<b>Authentication required</b>	<p>Optional proxy server credentials for logging on to the proxy server. You can enter credentials for the system proxy or for a custom proxy. Typically, you do not want users to have to log on to download updates.</p> <p><b>Note:</b> If your client computers use a proxy with authentication, you must specify trusted web domain exceptions for Symantec URLs. The exceptions let your client computers communicate with Symantec Insight and other important Symantec sites.</p> <p>For information about the recommended exceptions, see:  <a href="#">How to test connectivity with Insight and Symantec Licensing servers</a>.</p> <p><b>NT LAN Manager Authentication</b>  Additional optional authentication through NT LAN Manager (NTLM). You must include the domain name in the user name field, in the following format:  domain_name\user_name  The domain name cannot exceed 14 characters, and the user name cannot exceed 64 characters.  The names may not consist entirely of periods or spaces, nor can they contain the following characters: \ / " [ ] :   &lt; &gt; + = ; , ? * @</p> <p><b>Note:</b> If you select authentication for a system proxy or NT LAN Manager Authentication, any client versions earlier than 14.2 RU1 may lose communication.</p>

**Table 288: Proxy server options for Mac**

Option	Description
<b>Do not use a proxy server</b>	No proxy server is used.
<b>System proxy</b>	Use the proxy information that is entered into the browser on the client computers. In Safari, this information appears under <b>Safari &gt; Preferences &gt; Advanced &gt; Proxies</b> .
<b>Use custom proxy settings</b>	<p>Use the proxy server information address and the listening port that you enter here. Depending on whether you use the HTTP protocol or the HTTPS protocol, enter the port to use.</p> <ul style="list-style-type: none"> <li><b>Authentication required</b>  Optional custom proxy server credentials for logging on to the proxy server. Typically, you do not want users to have to log on to download updates.</li> </ul>

## LiveUpdate Server Settings for Mac clients

You use the Mac Server Settings pane in the LiveUpdate Settings policy to specify how Mac clients get content updates.

**Table 289: LiveUpdate Server Settings for Mac clients**

Setting	Description
<b>Use the default Symantec LiveUpdate server</b>	Downloads the content updates from the default Symantec LiveUpdate server over the Internet.
<b>Use a specified internal LiveUpdate server</b>	Downloads the content updates from an internal LiveUpdate server. You can specify multiple internal LiveUpdate servers for failover support. You can <b>Add</b> , <b>Edit</b> , and <b>Delete</b> LiveUpdate servers and use <b>Move Up</b> and <b>Move Down</b> to change the position of the LiveUpdate servers in the list.

## LiveUpdate Advanced Server Settings

If your internal LiveUpdate server uses FTP, you can set the type of FTP connection that you need to use. In Passive FTP, you control the port on which the FTP server connects to Symantec Endpoint Protection Manager. In Active FTP, the FTP server selects the port and then connects to Symantec Endpoint Protection Manager on that port. You may need to use Active FTP if the FTP server you use is behind a firewall, router, or network address translation device.

## LiveUpdate Policy: Mac Schedule

You use this page to specify how often to push updates from LiveUpdate servers to clients in the groups to which this policy is applied.

**Table 290: LiveUpdate schedule settings for Mac clients**

<b>Frequency</b>	Specifies how often to schedule clients to run LiveUpdate to download the latest updates. The default is <b>Every 4 hours</b> . The specific time option is available for both <b>Daily</b> and <b>Weekly</b> options. The specific day option is available for the <b>Weekly</b> setting only. The <b>Continuously</b> option only supports those clients that upgrade from versions earlier than 12.1.4. This setting gives those clients an hourly schedule. If you select <b>Continuously</b> for a client 12.1.4 or later, the client's previous LiveUpdate schedule remains. If the client had no previously specified schedule, then LiveUpdate runs on the default schedule.
<b>Download Randomization Options</b>	Specifies a randomization option. You can stagger the updates, plus or minus the value that is specified, to minimize the effect on network traffic. By default, Symantec Endpoint Protection randomizes the LiveUpdate sessions to minimize bandwidth spikes.

## LiveUpdate Policy Settings Mac Advanced Settings

(not available as of 14.3 RU2)

You can allow clients to receive product updates from a LiveUpdate server.

**Table 291: LiveUpdate Policy Settings Mac Advanced Settings**

Setting	Description
Product Update Settings	<p><b>Download Symantec Endpoint Protection product updates using a LiveUpdate server</b> Downloads and installs client software updates automatically when users click LiveUpdate or when a scheduled LiveUpdate session runs. When disabled, prevents downloading and installing client software updates, even if another Symantec product runs LiveUpdate on the client computer.</p> <p>If the LiveUpdate Settings policy specifies that clients download updates from a Symantec Endpoint Protection Manager or Group Update Provider, the updates are in the form of microdefs. If the LiveUpdate Settings policy specifies that clients download updates from a LiveUpdate server, the updates are in the form of MSP (patch) files.</p> <p>This setting lets you control client software versions. When this setting is disabled, client software can only be manually updated. When the management server downloads and processes patches, it creates a microdef, which automatically appears as a new package. The new package appears in the <b>Client Install Packages</b> pane. You must provide manual updates for Mac clients by using a third-party tool or by making the update package available for download on your network.</p>

## HTTP or HTTPS Proxy server settings

This dialog box lets you configure clients to use a proxy server for LiveUpdate communication. The client uses the settings that you configure in this dialog box only for LiveUpdate. You can configure a proxy server for other external communications separately.

**Table 292: HTTP or HTTPS proxy server options**

Settings	Options and Descriptions
HTTP or HTTPS Proxy Configuration	<ul style="list-style-type: none"> <li>• <b>I do not use a proxy server for HTTP or HTTPS</b> No proxy server is used.</li> <li>• <b>I want to use my Windows Internet Options proxy settings (default)</b> Use the proxy information that is entered into the browser on the client computers. This information appears in Internet Options &gt; Connections &gt; LAN Settings.</li> <li>• <b>I want to customize my HTTP or HTTPS settings</b> Use the proxy server address and the HTTP or HTTPS listening port on the server that you enter here.</li> <li>• <b>Authentication required</b> Optionally, use the custom proxy server authentication information that you enter here to log on to the server. <ul style="list-style-type: none"> <li>— You can use <b>Basic Authentication</b>, which requires the user name and password for the account that you want to use for the proxy server.</li> <li>— You can use <b>NT LAN Manager Authentication</b>, which requires the user name and password for the account that you want to use for the proxy server.</li> </ul> </li> </ul> <p><b>Note:</b> If you specify a proxy with authentication, you must create trusted web domain exceptions for Symantec URLs. The exceptions let your client computers communicate with Symantec Insight and other important Symantec sites.</p> <p>For information about the recommended exceptions, see:  <a href="#">How to test connectivity with Insight and Symantec Licensing servers.</a></p>

---

## FTP Proxy server settings

This dialog box lets you configure clients to use a proxy server for LiveUpdate communication. The client uses the settings that you configure in this dialog box only for LiveUpdate. You can configure a proxy server for other external communications separately.

**Table 293: FTP proxy server options**

Settings	Options and Descriptions
FTP Proxy Configuration	<ul style="list-style-type: none"><li>• <b>I do not use a proxy server for FTP</b> No proxy server is used.</li><li>• <b>Use the proxy server specified by the client browser (default)</b> Use the proxy information that is entered into the browser on the client computers. In Internet Explorer, this information appears in Internet Options &gt; Connections &gt; LAN Settings.</li><li>• <b>I want to customize my FTP settings</b> Use the proxy server information address and the listening port on the server that you enter here.</li></ul>

## LiveUpdate Server Settings for Linux clients

You use the Linux Server Settings pane in the LiveUpdate Settings policy to specify how Linux clients get content updates.

**Table 294: LiveUpdate Server Settings for Linux clients**

Setting	Description
Use the default Symantec LiveUpdate server	Downloads the content updates from the default Symantec LiveUpdate server over the Internet.
Use a specified internal LiveUpdate server	Downloads the content updates from an internal LiveUpdate server. You can specify multiple internal LiveUpdate servers for failover support. You can <b>Add</b> , <b>Edit</b> , and <b>Delete</b> LiveUpdate servers and use <b>Move Up</b> and <b>Move Down</b> to change the position of the LiveUpdate servers in the list. <b>Note:</b> Only the first ten internal LiveUpdate servers are included in the policy that is sent to the client. This includes any servers that you configured on a replication partner site.
LiveUpdate Proxy Configuration	Configure a proxy server to use for LiveUpdate from the default Symantec LiveUpdate server or from a specified internal LiveUpdate server. This proxy server is used only for LiveUpdate and not for any other external communications.

## LiveUpdate Advanced Server Settings for Linux clients

If your internal LiveUpdate server uses FTP, you can set the type of FTP connection that you need to use. In Passive FTP, you control the port on which the FTP server connects to Symantec Endpoint Protection Manager. In Active FTP, the FTP server selects the port and then connects to Symantec Endpoint Protection Manager on that port. You may need to use Active FTP if the FTP server you use is behind a firewall, router, or network address translation device.

## Proxy Server Settings for Linux clients

This dialog box lets you configure clients to use a proxy server over HTTP for LiveUpdate communication with Linux clients. The client uses the settings that you configure in this dialog box only for LiveUpdate. You can configure a proxy server for other external communications separately.

**Table 295: HTTP proxy server options**

Settings	Options and Descriptions
HTTP Proxy Configuration	<ul style="list-style-type: none"><li>• <b>I do not use a proxy server for HTTP</b> No proxy server is used.</li><li>• <b>I want to customize my HTTP settings</b> Use the proxy server address and the HTTP listening port on the server that you enter here.</li><li>• <b>Authentication required</b> Optionally, use the custom proxy server authentication information that you enter here to log on to the server.</li></ul> <p><b>Note:</b> If you specify a proxy with authentication, you must create trusted Web domain exceptions for Symantec URLs. The exceptions let your client computers communicate with Symantec Insight and other important Symantec sites.</p> <p>For information about the recommended exceptions, see: <a href="#">How to test connectivity with Insight and Symantec Licensing servers.</a></p>

## LiveUpdate Policy: Linux Schedule

You use this page to specify how often to push updates from LiveUpdate servers to Linux clients in the groups to which this policy is applied.

### NOTE

Do not uncheck **Enable LiveUpdate Scheduling**. If you disable **LiveUpdate Scheduling**, Linux clients cannot launch LiveUpdate to receive the latest updates.

**Table 296: LiveUpdate policy schedule options**

Option	Description
Frequency	Specifies how often to schedule clients to run LiveUpdate to download the latest updates. The default is <b>Every</b> 4 hours. The specific time option is available for both <b>Daily</b> and <b>Weekly</b> options. The specific day option is available for the <b>Weekly</b> setting only. The <b>Continuously</b> option allows the client computers that infrequently communicate with the Symantec Endpoint Protection Manager server to get the latest updates. They get the latest updates when they connect to the network and authenticate to the server.
Retry Window	Specifies the number of hours or days to keep trying to run LiveUpdate if the scheduled run of LiveUpdate failed for some reason. This option is enabled when the Every, Daily or Weekly option is selected. The default is a two-hour retry window.
Download Randomization Options	Specifies a randomization option. You can stagger the updates, plus or minus the value that is specified, to minimize the effect on network traffic. By default, Symantec Endpoint Protection randomizes the LiveUpdate sessions to minimize bandwidth spikes.

---

# LiveUpdate Content Policy

## Security Definitions

You can select the type of updates that can be installed on Symantec Endpoint Protection clients. For Windows computers, **Use latest available** specifies to install the latest update available from Symantec. **Select a revision** lets you test an update first before you install it on clients, and also lets you rollback to a previous version if necessary.

### NOTE

If you set the content type to **Select a revision** and then convert the Symantec Endpoint Protection client to a cloud-managed client, the content does not update on the client. To avoid this issue, make sure you set the content option to **Use latest available** before you convert the client.

The definitions and content types that you select must also be downloaded to the Symantec Endpoint Protection Manager if the management server is the only update provider. You specify what is downloaded to the management server with the local site server property settings for LiveUpdate.

Host Integrity content is only available to download from a LiveUpdate server to Symantec Endpoint Protection Manager and then to clients. Clients cannot download Host Integrity content directly from a LiveUpdate server.

Advanced machine learning content is only available for cloud-managed client groups with a Low-Bandwidth policy that enables low-bandwidth content. Standard and embedded clients use advanced machine learning content instead of standard definitions. Dark network clients do not use low-bandwidth mode.

[About the types of content that LiveUpdate downloads](#)

### NOTE

Mac client computers install updates only to the Virus and Spyware definitions and intrusion prevention signatures.

## LiveUpdate Content product updates

This dialog box lets you select LiveUpdate Content product updates for client software and is applied to the group. If this setting is enabled, you can restrict client computers from downloading and installing product updates when they run LiveUpdate. You make this restriction with a LiveUpdate Settings policy for each location in the group. If this setting is disabled, the LiveUpdate Settings policy for product updates and LiveUpdate has no effect.

## LiveUpdate Content Policy Settings for group name

This dialog box shows the currently applied LiveUpdate Content policy, and lets you apply a different policy to the group. LiveUpdate content policies apply to all locations in a group.

## Select revision

You can specify an older version of each content type based on the date. If you select a content revision from a specific date, then the clients in that group only download the content corresponding to that date.

Use this option for troubleshooting. You should temporarily roll back the content to a previous, safe version in the following cases:

- The current content version causes conflicts on the client computer.
- You want to test the latest content version before you apply it to all clients.

If **(none)** appears in the **Revision** column, one of the following issues have occurred:

- Symantec Endpoint Protection Manager is not configured to download that content type.

---

### Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager

- The revision in the policy does not match the revisions that are stored on the Symantec Endpoint Protection Manager. For example, you might import a policy that references a revision that does not exist on the server. Or, you might replicate policies but not LiveUpdate content from another site.
- You replicated this policy from a remote site, but you did not replicate the LiveUpdate content. The remote site stores the specified revision, but the local site does not.

Even though the revision is not available on the server, the clients that use the policy are still protected. The clients use the latest revision of the content.

## Replace LiveUpdate Content policy

This dialog box lets you replace one LiveUpdate Content policy with another LiveUpdate Content policy. LiveUpdate Content policies affect all locations in a group.

The selected policy is shown as the **Old LiveUpdate Policy**; select the policy to replace it using the drop-down list for **New LiveUpdate Policy**.

Under **Replace Policy**, the tree shows the groups from which you can replace the policy. Check the box next to a group to select it. To select all subgroups, right-click the parent group and choose **Select All Subgroups**.

## Select an engine version

Symantec Endpoint Protection contains several engines that carry out parts of its functionality. These engines are binary files (.dll or .exe) and are delivered with the security definitions.

This option locks the clients to one particular engine, but continues to distribute the latest security definitions that are associated with that engine. Use this option if you know the current engine works in your environment, and you need to test the latest engine before you release it.

For finer-tuned control, click **Use latest version** so that the clients receive the latest version of both the engine and the security definitions. For example,

Clients earlier than 14.0.1 MP1 ignore this setting. Instead, they download the latest version of the content. If you have a mixed group of 14.0.1 MP1 and legacy clients, and specify an engine version, legacy clients always receive the latest engine content.

### NOTE

If two engine updates are released the same day, they have the same date format.

Symantec Endpoint Protection Manager only keeps the latest three revisions of the content per each engine version.

Some content types do not have an engine component, only security definitions. In that case, the **Select an engine version** option is disabled. No engine content exists for the Symantec Allow List (Symantec Whitelist), Revocation Data, Reputation Settings, Submission Control Data, Extended File Attributes and Signatures, and the AP Portal List.

## Admin page

The Admin page includes topics about licenses, administrators, and domains. Look for information about licenses only in this chapter.

## License Renewal

When you renew, select the old license before you activate the new license. This step in the renewal process ensures that the system deletes the old license and replaces it with the new license.

## License Main Page

Use this page to view and manage licenses for Symantec Endpoint Protection.

**Table 297: License overview options**

Option	Description
<b>Licenses</b>	<p>Lists license serial number, number of seats, and expiration date for each product license on the server. Click a license in the tree view to see more information for the license in the main window.</p> <p><b>The information for each license includes:</b></p> <ul style="list-style-type: none"><li>• <b>Serial Number</b></li><li>• <b>Type</b></li><li>• <b>Seats</b></li><li>• <b>Start Date</b></li><li>• <b>Expiration Date</b></li><li>• <b>Action</b></li></ul>
<b>Tasks</b>	<p><b>These are the tasks associated with licensing:</b></p> <ul style="list-style-type: none"><li>• <b>Activate license</b> You activate your license by entering the license serial number or by importing a Symantec License file (.slf). Clicking this task starts the License Activation wizard where you enter the serial number or select the .slf file. You also use this task to add additional licenses and renewal licenses.</li><li>• <b>Edit Partner Information</b> Use this task to enter partner information. A partner is someone who maintains the product licenses on your behalf, such as a systems integrator, consultant, or a preferred reseller.</li><li>• <b>Purchase additional licenses</b> This task takes you to the Symantec website to purchase additional licenses.</li></ul>

[Licensing Symantec Endpoint Protection](#)

## Upgrade license help

When you upgrade from 12.1.x, Symantec Endpoint Protection 14.x does not require a new license. You use your existing 12.1.x license, which displays the 12.1 version. When you renew your contract and your license, then you receive a 14.x license.

A direct upgrade from Symantec Endpoint Protection Manager 11.x directly to 14.x is not supported. If you first upgrade from 11.x to 12.1.x. and then to 14.x, you import your 14.x license at that time.

Answers to licensing questions and instructions for solving most upgrade licensing issues are available at [Maintenance entitlement overview for Symantec Endpoint Protection](#).

[Supported upgrade paths to the latest version of Symantec Endpoint Protection 14.x](#)

[Activating or importing your Symantec Endpoint Protection product license](#)

## Clients: Clients

Use this tab to view a list of clients in the selected group. You can also view information about each client, including general computer and protection status information.



---

Viewing the protection status of client computers

**Table 298: Clients tab status view options**

Column	Description
Default view	<p><b>Displays the following information:</b></p> <ul style="list-style-type: none"> <li>• <b>Name</b> The host name of the computer and the icon that matches the computer type.</li> <li>• <b>Health State</b> Whether or not the client computer is connected to the management server, the client is infected, or there are any pending Power Eraser detections that require administrator action.</li> <li>• <b>Logon User or Computer</b> The account that is associated with the installed client.</li> <li>• <b>Last Time Status Changed</b> The date and time when the client status last changed after server check-in.</li> <li>• <b>Virus Definitions</b> The date and the revision number of the latest virus and spyware definitions file.</li> <li>• <b>Policy Serial Number</b> The serial number that uniquely identifies the current version of the policy that applies to the selected group. You should check the policy serial number on the client to see if it matches the serial number that appears in the console. If the client communicates with the management server and receives regular policy updates, the serial numbers should match.</li> <li>• <b>Last Scan Started</b> The last date and time that a full disk scan was performed. A full scan scans the entire computer for viruses and security risks, including the boot sector and system memory. The client should run a full scan once a week.</li> <li>• <b>AntiVirus Status</b> The state of Auto-Protect. Auto-Protect is either enabled or disabled. Auto-Protect protects both the file system and the email attachments that clients receive.</li> <li>• <b>Firewall Status</b> The state of firewall, which is either enabled or disabled.</li> <li>• <b>Low Bandwidth</b> This option indicates whether Low Bandwidth content is enabled. This column only appears after Symantec Endpoint Protection Manager enrollment with the cloud console.</li> <li>• <b>Restart Required</b> The indication that the client must be restarted is either yes or no. If you recently installed a new computer with the client software, the client computer must be restarted.</li> <li>• <b>Description</b></li> </ul>
Client status	<p><b>Displays the following information:</b></p> <ul style="list-style-type: none"> <li>• <b>Name</b> The host name of the computer and the icon that matches the computer type.</li> <li>• <b>Health State</b> Whether or not the client computer is connected to the management server, the client is infected, or there are any pending Power Eraser detections that require administrator action. The status message <b>Online</b> indicates a connected client, and <b>Offline</b> indicates a disconnected client. The message <b>Alert</b> indicates either pending infection detections, or pending Power Eraser detections. Clients that connect through Symantec Endpoint Protection Manager may not immediately display the correct online status in the cloud console. Allow for 5-10 minutes after the online status changes to see an accurate reflection of the current status.</li> <li>• <b>Logon User or Computer</b> The account that is associated with the installed client.</li> <li>• <b>IP Address</b> The IP address of the host computer.</li> <li>• <b>Client Version</b> The version number of the client software.</li> <li>• <b>Last Time Status Changed</b> The date and time when the client's status last changed after it checked in with the server.</li> <li>• <b>Restart Required</b> The indication that the client must be restarted is either yes or no. If you recently installed a new computer with the client software, the client computer must be restarted.</li> <li>• <b>Policy Serial Number</b> The serial number that uniquely identifies the current version of the policy that applies to the selected group.</li> </ul>

Column	Description
<b>Protection technology</b>	<p><b>Displays the following information:</b></p> <ul style="list-style-type: none"> <li>• <b>Name</b> The host name of the computer.</li> <li>• <b>Health State</b> Whether or not the client computer is connected to the management server, the client is infected, or there are any pending Power Eraser detections that require administrator action.</li> <li>• <b>Logon User or Computer</b> The account that is associated with the installed client.</li> <li>• <b>IP Address</b> The IP address of the host computer.</li> <li>• <b>Last Scan Started</b> The last date and time that a full disk scan was performed. A full scan scans the entire computer for viruses and security risks, including the boot sector and system memory. The client should run a full scan once a week.</li> <li>• <b>&lt;protection name&gt; Status</b> The status of the protection feature, either enabled or disabled. <ul style="list-style-type: none"> <li>– <b>Not reporting status</b> means that the client does not communicate with Symantec Endpoint Protection Manager.</li> </ul> </li> <li>• <b>&lt;protection name&gt; Definitions</b> The date and the revision number of the latest definitions file installed on the client computer. Not available means that the definitions have not been downloaded to Symantec Endpoint Protection Manager.</li> <li>• <b>Status</b></li> </ul>
<b>Network information</b>	<p><b>Displays the following information:</b></p> <ul style="list-style-type: none"> <li>• <b>Name</b> The host name of the computer.</li> <li>• <b>Health State</b> Whether or not the client computer is connected to the management server, the client is infected, or there are any pending Power Eraser detections that require administrator action.</li> <li>• <b>Domain/Workgroup</b> The domain or workgroup to which the client computer belongs.</li> <li>• <b>Logon User or Computer</b> The account that is associated with the installed client.</li> <li>• <b>IP Address</b> The IP address of the host computer.</li> <li>• <b>DNS Server</b> The host name or IP address of the DNS server.</li> <li>• <b>WINS Server</b> The host name or IP address of the WINS server.</li> <li>• <b>MAC Address</b> The MAC address of the network card that the computer uses.</li> <li>• <b>Gateway</b> The host name or IP address of the gateway that the computer uses.</li> </ul>

Column	Description
Client system	<p><b>Displays the following information:</b></p> <ul style="list-style-type: none"> <li>• <b>Name</b> The host name of the computer.</li> <li>• <b>Health State</b> Whether or not the client computer is connected to the management server, the client is infected, or there are any pending Power Eraser detections that require administrator action.</li> <li>• <b>Logon User or Computer</b> The account that is associated with the installed client.</li> <li>• <b>IP Address</b> The IP address of the host computer.</li> <li>• <b>Operating System</b> The computer's operating system, such as Windows 10.</li> <li>• <b>Service Pack/Build number</b> The operating system's service pack number, such as Service Pack 2.</li> <li>• <b>Free Memory</b> The approximate amount of available memory on the computer, in MB.</li> <li>• <b>Free Disk Space</b> The approximate amount of available disk space on the computer, in MB.</li> <li>• <b>Total Disk Space</b> The approximate amount of total disk space (the maximum disk capacity), in MB.</li> </ul>

## Clients: Policies

The main tasks that you can perform on this tab are related to non-shared and shared policies for specific locations of a group. You can also set a number of advanced security settings.

**Table 299: Policy inheritance and location-independent policies and settings**

Option	Description
Inherit policies and settings from parent group	<p>In a hierarchical structure, subgroups automatically inherit information about locations and policies from a group that is located higher than the subgroup. By default, the inheritance is enabled for every group. This option only appears when you select any group other than the My Company group.</p> <p>The policy inheritance setting does not apply to policies from the cloud. You identify the cloud-based policies by the cloud icon that appears next to the policy description. The cloud icon indicates that the policy applies directly to the group. The cloud icon with an arrow indicates that the group inherits the policy from its parent in the cloud console.</p>
Custom Intrusion Prevention	Enables you to assign a custom IPS library to a group rather than an individual location. You can later assign additional custom IPS libraries to the group.
System Lockdown	System Lockdown enables you to control the applications that users can run on a client. Client software includes a tool that is called checksum.exe. Use this tool to create a file fingerprint list. The file fingerprint list contains checksum and location information. This information applies to applications that you can approve or deny for use at your company.
Network Application Monitoring	<p>When network application monitoring is enabled, the client monitors the applications that run on the client to detect any changes. For example, a user can decide to replace a specific version of an application. This action is detected. You can also ask the user for permission to block the installation of this application. Finally, you can also log the action.</p> <p>You can create an Exception List for the applications that you do not want to monitor. Applications that you add to the <b>Unmonitored Application</b> list are not monitored.</p>

Option	Description
LiveUpdate Content Policy Settings	Shows the currently applied LiveUpdate Content policy. You can apply a different policy to a specific group.
Client Log Settings	Client log settings are used to enable the uploading of log information from the clients to the manager. You can also set the size, the time of retention, and the damper options for the upload the cache that is used on the clients. These settings apply to all the clients in the group.
Communications Settings	Displays the communications settings of the selected management server. These settings include the name of the management server list. You can specify whether to use the push or pull mode to download policies from the management server to the client. You can specify whether you want information about the use of applications to be sent to the management server. You can set the frequency with which the management server uploads information from the client and the client downloads information from the management server.
External Communication Settings	Displays the communications settings for submissions, tamper protection, and proxy servers. You can enable your clients to submit file reputation, antivirus detection, and SONAR detection information about detected threats to Symantec Security Response. Symantec Security Response uses this information to improve Symantec's ability to respond to threats and customize protection. Symantec recommends that you enable your client computers to submit this information. You can configure Windows and Mac clients to use no proxy server, the default proxy server that is defined on the client computer, or a custom HTTPS server.
General Settings	On the <b>Restart Settings</b> tab, you can specify how Symantec Endpoint Protection is restarted on the client computers when it is installed or upgraded. On the <b>General Settings</b> tab, you can configure location settings and restart options for client computers. On the <b>Security Settings</b> tab, you can specify whether passwords are required for users under certain circumstances. You can also specify whether a digital certification is required for authentication. You can also block all traffic unless a firewall is active. On the <b>Tamper Protection</b> tab, you can tighten the security for Symantec's security software. You can block an attempt to tamper with the client, or you can log the attempt. You can specify a message that alerts the user in the case of any tampering. These settings are inherited. You cannot edit these settings at the group level.

## Clients: Details

Use this pane to review details about the selected group or the selected subgroup.

**Table 300: Details pane information**

Row name	Description
Group Name	The name of the selected group.
Description	The description of the selected group.
Full Path Name	The full path of the selected group, including the group name.
Number of Physical Computers	The number of physical computers that were added to the selected group.
Number of Registered Users	The number of registered users in the selected group.
Created by	The user name of the administrator who created the selected group.
Created	The date and the time when the selected group was created.
Last Modified	The date and the time when the selected group was last modified.
Block New Clients	The indicator of whether the selected group accepts new clients. Displays Yes or No.
Policy Serial Number	The unique serial number of the selected group's policy.

Row name	Description
Policy Date	The date and the time when the policy was last updated.
Custom Intrusion Prevention Serial Number	The name of the custom fingerprint library that was used.

## Install Packages

This pane displays a list of client installation packages assigned to the selected group.

**Table 301: Install Packages**

Column	Description
<b>Package Name</b>	The name of the client installation package.
<b>Type</b>	The type of client installation package.
<b>Version</b>	The version of the client installation package.
<b>Start Time</b>	The date and the timestamp of when the client installation package was assigned to the group.
<b>Available</b>	A check in this column indicates that the package is available.

[Upgrading client software with AutoUpgrade](#)

## Select Scan Type

You can select the type of on-demand scan that you want to run for a group you select in the tree view.

### NOTE

Only a custom scan is available for Mac clients. If you run an active scan or a full scan on a group that includes Mac clients, the Mac clients run a custom scan.

**Table 302: Types of on-demand scans**

Type of scan	Description
<b>Active Scan</b>	Quickly scans system memory and the locations that viruses and security risks commonly attack.
<b>Full Scan</b>	Scans the entire computer, including the boot sector and system memory.
<b>Custom Scan</b>	Uses the settings for the on-demand scans that are configured in the Virus and Spyware Protection policy for the selected computer or group. By default, these settings include scanning all folders and file types. You can configure the custom scan to scan only particular files and folders. You can configure the settings that you want in the policy for the client or the group. Then you can run the custom scan with these settings.

## Add Group for group name

Use this dialog box to add a new group to the selected group or subgroup. A group name must contain a maximum of 990 characters. The full path of the group name must contain a maximum of 1000 characters. You cannot use the following characters: " / \ \* ? < > | : &

You cannot add a subgroup to the **Default Group**.

[Managing groups of clients](#)

---

## Add Computer for group name

You can add a new client in computer mode to protect the computer regardless of who logs on to the computer. In computer mode, the client gets the policies from the group to which the computer belongs. The client protects the computer with the same policies, regardless of which user is logged on to the computer.

**Table 303: Add Computer options**

Option	Description
<b>Computer Name</b>	The computer name or full computer name.
<b>Domain</b>	Either the Windows Domain name or Workgroup. You must know the computer name and the Windows Domain name before you can add a client. If the computer is not part of a Windows Domain, it is part of a Windows Workgroup. The maximum length of the domain name is 32 characters.
<b>Description</b>	An optional description that gives additional details about the computer. All characters are allowed. The maximum length of the description field is 256 characters.

## Add User for group name

You can add a client in user mode so that the client gets the policies from the group to which the user belongs. The policies that are applied to the client computer change, depending on the user who is logged on to the computer at the time. You might also want to use user mode for users who log on to multiple client computers.

You must know the user name and whether the user is part of which Windows Domain name or a workgroup to add a client.

**Table 304: Add User options**

Option	Description
<b>User Name</b>	The unique user name for the user who logs on to the client computer.
<b>Domain Name</b>	The user is part of either a Windows Domain or the Windows Workgroup. <b>You must specify one of the following options:</b> <ul style="list-style-type: none"><li>• <b>Log on domain</b> The Windows Domain name</li><li>• <b>Log on local computer</b> The Windows Workgroup</li></ul>
<b>Description</b>	An optional description that gives additional details about the user. The description can be up to 256 characters long. All characters are allowed.

## Integrate with Organizational Unit Tree

Use this dialog box to import organizational units or containers from an Active Directory server or an LDAP server.

You cannot place an organizational unit in more than one group tree.

This process may take time, depending on the number of users in the unit or container.

**Table 305: Options when you import an Organizational Unit or container**

Option	Description
Domain	The domain of the server that is the host to Active Directory or LDAP.
Refresh	Refresh the organizational unit structure content or container content.

## Search Clients

Use this dialog box to search for information about one or more clients in a group. For example, you might want to know which client computers have the latest policy file.

The data query tool provides predefined search criteria, comparison operators, and values. The data query combines search conditions using the Boolean AND logic. After you display the results, you can export them into a text file.

To collect information about the users, click **Admin > Install Packages > Set User Information Collection**.

**Table 306: Searching for computers options**

Option	Description
<b>Find</b>	Searches for client computers based on whether the client is in computer mode or user mode. <b>In Group</b> displays the group that you selected in the <b>Clients</b> tree view.
<b>Search Criteria</b>	Displays a list of attributes about the client, client computer, or user. To see the available list, you can click in the empty cell under <b>Search Field</b> . You can select the search criterion you want to use from the drop-down menu.
<b>Comparison Operator</b>	Displays a list of operators. You can click the empty cell under <b>Comparison Operator</b> , and then select one of the following operators from the drop-down menu: <ul style="list-style-type: none"><li>• <b>= (equal to)</b></li><li>• <b>!= (not equal to)</b></li><li>• <b>&gt; (greater than)</b></li><li>• <b>&lt; (less than)</b></li><li>• <b>&gt;= (greater than or equal to)</b></li><li>• <b>&lt;= (less than or equal to)</b></li><li>• <b>LIKE</b></li></ul> Places a wildcard "%" character at both the beginning or the end of the string you typed. The query then locates any strings that begin with, end with, or contain the value you typed.
<b>Value</b>	Enables you to enter a new value or select a predefined value. You can click the empty cell under <b>Value</b> to enter a string to search on. The search criterion you selected in the <b>Search Field</b> column determines the value that you should type. Strings are not case sensitive. You can use the LIKE operator to match a partial entry, as explained for <b>Comparison Operator</b> .
<b>Export</b>	Saves the contents of the query in a text file.

## Export Communications Settings for group name

You may need to create a new client-server communications file, and replace it on the client for the following reasons:

- To reestablish the connection between the client and the server.
- To change the group that a client is in.
- To convert an unmanaged client to a managed client.
- To convert a managed client to an unmanaged client.

The communication file is used to register a client computer to a specific group and to connect to the management server.



---

### This file contains the following settings:

- The management server that the client computer should connect to.
- Whether the management server pushes or pulls the policy file to or from the client.
- The frequency in which clients upload data if the client pulls the policy file.
- The group in which the converted client is placed.

After you export the communications file to the client computers, you must import it on the client. The default file name is group name\_symlink.xml.

**Table 307: Options for exporting the group communications settings**

Option	Description
<b>Export To</b>	Specifies the location to save the file, either on your computer or on the location. The default file name is group name_symlink.xml.
<b>Preferred Policy Mode</b>	<b>Specify whether you want the policies for this group to apply to the computers in the group or the users in the group:</b> <ul style="list-style-type: none"><li>• <b>Computer mode</b> Specifies that the policies apply to computers as they authenticate to the management server.</li><li>• <b>User mode</b> Specifies that the policies apply to users as they log on to computers and authenticate to the management server.</li></ul>

## Group Properties

The Group Properties dialog displays summary information for the selected group. You can edit a group's description and you can block new clients from the group.

**Table 308: Group Properties options**

Option	Description
<b>Group ID</b>	Identification number for the group.
<b>Name</b>	The group name as it appears in the View tree.
<b>Description</b>	The description of the group. This field is optional and is for informational purposes only.
<b>Full Path Name</b>	The full path to the selected group.
<b>Number of Physical Computers</b>	The number of computers in the selected group.
<b>Number of Registered Users</b>	The number of users in the selected group.
<b>Created By</b>	The name of the administrator who created the selected group.
<b>Created</b>	The date and time at which the group was created.
<b>Last Modified</b>	The date and time at which the group was last modified.
<b>Policy Serial Number</b>	The automatically-generated serial number for the policy that is in effect.
<b>Policy Date</b>	The policy creation date and time stamp.
<b>Custom Intrusion Prevention Serial Number</b>	The automatically-generated serial number for the Custom Intrusion Prevention Signatures policy that is in effect.
<b>Block New Clients</b>	When enabled, blocks users and computers from automatically being added to a group. By default, this option is disabled.

[Managing groups of clients](#)

---

## Set Display Filter

Use this dialog box to filter the clients that are displayed for the group that you have selected.

### NOTE

The Symantec Endpoint Protection Manager retains the filter setting and stores it with the logon name of the individual administrator or limited administrator. If an administrator sets a filter condition, that condition is retained for that administrator. Different administrators see only the filters that they have set themselves.

**Table 309: Display filter options**

Option	Description
<b>Platform type</b>	Displays the computers that run the Windows client, the Mac client, or the Linux client. You can also display all clients at once.
<b>Client type</b>	Displays the client computers based on the type of account the clients have. You configure the clients with a user account or a computer account, based on how you want to apply policies to the clients in group. <a href="#">Switching a Windows client between user mode and computer mode</a>
<b>New users or computers that have been created but that don't yet have the client software installed</b>	Check to display the computers that have already been added with a user account or computer account, but that don't have the client installed on them. You can use this list to determine which computers still need the client.
<b>Exclude offline non-persistent VDI clients</b>	Check to exclude from display the non-persistent clients that are offline in Virtual Desktop Infrastructures.
<b>Results per page</b>	Sets the maximum number of clients that you want to have displayed per page. You can display up to 999 computers.

## Add Unmanaged Detector Exception

Use this dialog box to configure an exception. You can use an IP address range or a specific MAC address.

**Table 310: Unmanaged Detector Exception options**

Option	Description
Exclude detection of an IP address range	The starting IP address and ending IP address of the range of addresses that you want to exclude from detection.
Exclude detection of a MAC address	The MAC address of the device you want to exclude from detection.

## Unmanaged Detector Exceptions

An unmanaged detector detects all devices on your network. Use this dialog box to specify devices to exclude from detection as unmanaged devices. For example, you might not want to include the devices that never run the client software, such as printers.

---

## Import LDAP Users

Displays the number of the Active Directory or LDAP users that you imported.

## Clients: Properties

You can view the client properties for more detailed information about its hardware, software, network, and user information.

All information that is displayed in these tabs is valid as of the last successful check-in to the management server.

[Set User Information Collection](#)

**Table 311: The General tab**

Value	Description
<b>Description</b>	A description for the client computer, which can be customized within the Symantec Endpoint Protection Manager.
<b>Computer Name</b>	The name of the client computer.
<b>Logon User Name</b>	The computer account that was logged on.
<b>Group</b>	The client group within the management server in which this client computer belongs.
<b>Domain or Workgroup</b>	The Windows domain or workgroup to which this client computer belongs.
<b>Computer Description</b>	The computer description as defined within the client computer system properties.
<b>Processor</b>	The number, family, and speed of the processor or processors.
<b>Memory</b>	The total amount of physical memory reported. See the <b>Clients</b> tab for the free memory total.
<b>BIOS Version</b>	The type and version of the BIOS.
<b>Operating System</b>	The operating system (platform and version).
<b>Kernel</b>	The kernel version of the installed operating system on this computer. Applies only to Linux computers. Appears blank for Windows or Mac clients.
<b>Service Pack</b>	The service pack reported.
<b>TPM Device</b>	The type of Trusted Platform Module (TPM) hardware device, if present.
<b>Unique ID</b>	The unique identifier for this installation of the Symantec Endpoint Protection client, created at the time of installation. The unique ID identifies the computer uniquely in the database.
<b>Hardware Key</b>	The unique identifier for the hardware configuration of this client computer.
<b>UUID</b>	The unique identifier for the BIOS of the computer. You might use the BIOS UUID for asset inventory or some other similar task.
<b>Operating System Language</b>	The language of the installed operating system.
<b>Total Disk Space</b>	The total amount of disk space on the computer. See the <b>Clients</b> tab for free disk space total.
<b>Group Update Provider</b>	Displays whether or not the client computer is a Group Update Provider.
<b>Deployment status</b>	Displays whether the deployment and the installation have succeeded or failed.
<b>Deployment message</b>	Displays the messages that the Symantec Endpoint Protection client returns after installation.
<b>Deployment target version</b>	The version of the Symantec Endpoint Protection client that is intended for deployment.
<b>Deployment running version</b>	The current version of the Symantec Endpoint Protection client.
<b>Last deployment time</b>	When the Symantec Endpoint Protection client was last deployed.

Value	Description
<b>Virtualization Platform</b>	The platform on which virtual client computers are hosted, such as VMware. Non-virtual client computers report "N/A".
<b>Serial Number</b>	For virtual machines, shows the VMware serial number.
<b>Install Type</b>	Shows whether the Symantec Endpoint Protection client is a standard client, embedded or VDI client, or dark network client. For legacy clients, shows whether the client is standard-size or reduced-size.
<b>Write Filters Status</b>	Whether or not Windows write filters are installed on this client.

**Table 312: The Network tab**

Value	Description
<b>Last Connected IP</b>	The IP address that was reported when the client computer last connected to the management server. If your environment uses network address translation (NAT), then this value may differ from <b>IP Address</b> .
<b>DHCP Server</b>	The DHCP server to which the client computer connects.
<b>DNS Servers</b>	The DNS server or servers to which the client computer connects.
<b>WINS Servers</b>	The WINS server or servers to which the client computer connects.
<b>Addresses</b>	<p>The different types of addresses that the client computer reports. There may be more than one of each kind of address.</p> <ul style="list-style-type: none"> <li>• <b>IP Address</b> The IP address.</li> <li>• <b>MAC Address</b> The unique network interface address that is associated with that IP address.</li> <li>• <b>Default Gateway</b> The default gateway in use.</li> </ul>

**Table 313: The Clients tab**

Value	Description
<b>Client</b>	The type of client installation reported.
<b>Client Software Version</b>	The Symantec Endpoint Protection build version.
<b>Client Security Patch Version</b>	The Symantec Endpoint Protection client security patch version. <a href="#">Downloading Endpoint Protection security patches to Windows clients</a>
<b>Current Policy Serial Number</b>	The serial number of the current management server policy in use.
<b>Virus Definitions</b>	The date and the revision number of the virus definitions in use.
<b>SONAR Definitions</b>	The date and the revision number of the SONAR definitions in use.
<b>IPS Definitions</b>	The date and the revision number of the intrusion prevention signature definitions in use.
<b>Download Protection Definitions</b>	The date and the revision number of the Download Insight definitions in use.
<b>EDR Definitions</b>	The date and the revision number of the Endpoint Detection and Response (EDR) product content. EDR provides forensic information to EDR servers. These definitions are updated by LiveUpdate.
<b>CNT Library and Configuration</b>	The date and revision number of the Common Network Transport Library and Configuration that Endpoint Detection and Response uses.
<b>AML Static Content</b>	The status of AML Static Content.

Value	Description
<b>WTR Definitions</b>	The date and the revision number for Web and Cloud Access Protection. Web and Cloud Access Protection protects Windows and Mac client computers against web-based threats.
<b>Host Integrity Status</b>	The status of the Host Integrity check, either <b>Success</b> or <b>Disabled</b> .
<b>Host Integrity Reason Code Description</b>	The description for the Host Integrity check status.
<b>Last Time Status Changed</b>	The last time the client reported a status change.
<b>Time Zone Offset</b>	The number of hours the time zone is offset from Greenwich Mean Time (GMT).
<b>Free Memory</b>	The available memory on the client computer.
<b>Free Disk Space</b>	The available hard disk space on the client computer.
<b>Memory Exploit Mitigation Status</b>	Whether Memory Exploit Mitigation is enabled. You can enable Memory Exploit Mitigation in the Intrusion Prevention policy.
<b>Low Bandwidth</b>	The status of Low Bandwidth. You must enroll Symantec Endpoint Protection Manager with the cloud console to use Low Bandwidth.
<b>Intensive Protection Status</b>	The status of Intensive Protection. You must enroll Symantec Endpoint Protection Manager with the cloud console to use Intensive Protection.
<b>Web and Cloud Access Protection Status</b>	Displays the Web and Cloud Access Protection status: <ul style="list-style-type: none"> <li>• <b>Enabled:</b> Web and Cloud Access Protection is installed and enabled on the computer.</li> <li>• <b>Not Installed:</b> Web and Cloud Access Protection was not installed as part of the Client Install Feature Set in the installation package.</li> <li>• <b>Disabled by policy.</b> The Web and Cloud Access Protection policy is not enabled for the clients in this group.</li> <li>• <b>Malfunctioning:</b> Web and Cloud Access Protection is not running correctly. Either the PAC URL is incorrect, or the token is invalid.</li> </ul> Web and Cloud Access Protection requires a license for Symantec Web Security Services. The Integrations policy was renamed to the Web and Cloud Access Protection policy in 14.3 RU1.
<b>Web and Cloud Access Protection Message</b>	Displays the Web and Cloud Access Protection Status in the Web and Cloud Access Protection log in the client.
<b>IPS Out-of-band Scanning Status</b>	Out-of-band scanning changes the processing model for networking traffic and may have compatibility issues with other Windows Filtering Platform (WFP) drivers. Therefore, if you enable this option, Symantec recommends that you test out-of-band scanning before you deploy it to your production environment. Performance characteristics vary depending on the workload.
<b>Endpoint Threat Defense for AD Status</b>	Symantec Endpoint Threat Defense for Active Directory (AD) effectively controls the attacker's perception of the organization's internal resources—all endpoints, servers, users, applications, and locally stored credentials. This solution autonomously learns the organization's Active Directory structure in its entirety and uses this data to create an authentic and unlimited obfuscation. Added in 14.2 RU1.
<b>URL Enabled Status</b>	URL Reputation in the IPS policy identifies threats from domains and URLs, which can host malicious content like malware, fraud, phishing, and spam. URL Reputation lets you block access to the web addresses that are identified as known sources of the malicious content.
<b>Browser (IE/FF/Chrome) Enabled Status</b>	These browser extensions provide better protection for both HTTP and HTTPS traffic to and from the Google Chrome, Internet Explorer, or Firefox web browsers. The Symantec Endpoint Protection client blocks users from accessing malicious websites from these browsers. The browser extension depends on IPS; therefore, the IPS policy must be enabled and assigned to the group. The browser extension is downloaded from LiveUpdate by default if the computer joined an Active Directory domain. Otherwise, the browser extension is downloaded from the Google Web Store. You enable or disable this content by clicking <b>Admin &gt; Servers &gt; Edit Site Properties &gt; LiveUpdate tab &gt; Content Types to Download &gt; Browser Extension</b> .

## Management server lists

### Add Management Server

You can specify the IP address or host name of the Symantec Endpoint Protection Manager. You can also customize the port numbers for both encrypted and non-encrypted communication between a management server and its clients.

**Table 314: Add Management Server dialog box**

Option	Description
Server address	Enables you to add or edit the IP address or host name of the management server. If you specify the IP address or host name of the management server, it is included in the management server list. IP address includes IPv4 and IPv6. For IPv6, you do not need to enclose the address with square brackets. The management console automatically adds the square brackets when needed.
Customize HTTP port	Enables you to customize the port number with which clients use to connect with a management server. The default TCP port number for HTTP is 8014.
Customize HTTPS port	Enables you to customize the port number with which clients use for an encrypted connection with a management server. The default TCP port number for HTTPS is 443. As of 14, Symantec Endpoint Protection Manager installs new installations with the HTTPS protocol by default.

### Management server list name: Assigned Groups and Locations

You can use this dialog box to view which groups the selected management server list is assigned to. The group icons with the selected management server icon display a white check mark. The groups that are unavailable (grayed out) inherit from a parent group.

### Management Server Lists

You can create a customized management server list to specify the order in which clients in a particular group connect to a server.

**Table 315: Management server list options**

Option	Description
Name and Description	Lists the name and description of the default management server list for the default site after the initial installation. If any management server lists are added, it displays the name and description of the management server list that you selected in the <b>Management Server Lists</b> pane.
Use HTTP protocol	Specifies whether to communicate by using the HTTP protocol. The default TCP port number for HTTP is 8014.
Use HTTPS protocol	Specifies whether to communicate by using the HTTPS protocol with the server that runs Secure Sockets Layer (SSL). The default TCP port number for HTTPS is 443. You can also use HTTPS protocol rather than the default HTTP protocol for communication. In addition, you can also customize the HTTP and HTTPS port numbers by creating a customized management server list. However, you must customize the ports before any clients are installed. Otherwise, the client-to-server communication is lost. If you change the protocol or the port numbers of the management server, you must edit them in the management server list. Clients can then resume communication. As of 14, Symantec Endpoint Protection Manager installs new installations with the HTTPS protocol by default.
Verify certificate when using HTTPS protocol	Requires the client to verify a certificate with a trusted third-party certificate authority.

Option	Description
Management Servers	<p>Displays the priority and IP address or host name of the management server. The priority and IP address are listed in the default management server list for the default site after initial installation. If any management server lists are added, the following happens: This text box also displays the priority and IP address or host name of management servers in the management server list. You selected the priority and IP address in the <b>Management Server Lists</b> pane.</p> <p>You can set priorities and add as many management servers as you want to each priority. Clients try to connect to management servers that are listed with a higher priority in a management server list first. You may want to perform this task before you deploy any clients. If multiple management servers are added at the same priority, clients can connect to any of the management servers at that priority. Clients automatically balance the load between the available management servers that have the same priority.</p>

## Replace Management Server List

You can apply a different management server list to groups by either assigning the selected list or by replacing one specific list with one other specific list. For example, suppose you have three lists, **Default Management Server List**, List2, and List3. You can replace **Default Management Server List** with List3, but you cannot replace List2 with List3 at the same time. You can replace both **Default Management Server List** and List2 at the same time by using the **Assign the List** command.

**Table 316: Replacement of a management server list**

Option	Description
<b>Old Management Server List Name</b>	The current management server list for the site.
<b>Old Management Server List Name</b>	The names of all management server lists that you can choose from to replace the <b>Old Management Server List</b> .
Check boxes of groups and locations	Enables you to check or uncheck any group for which you want to replace a management server list. The group names that appear in bold display the current management server list. You cannot replace a list for a group that inherits from a parent group. Groups that inherit display the following text: <b>[inherit from the parent group]</b> .
<b>Replace</b>	Replaces the old management server list with the new management server list for those groups and locations that you checked.

## Apply Management Server List

After you have created a management server list, you must apply it to one or multiple groups or locations for the management server list to become effective.

**Table 317: Applying a management server list to a group or location**

Option	Description
Management Server list	Displays the name of the management server list that you want to apply to the groups and locations.
Check boxes of groups and locations	Specifies the group and locations to which you want to apply the management server list. Groups or locations in bold already have the displayed management server list applied to them.
<b>Assign</b>	Applies the management server list to the selected groups or locations.

## Clients Page > Policies tab

### Communications Settings for <group\_name>

Use the Communications Settings dialog box to configure the communication between the management server and the client.

**Table 318: Management server and client communications settings**

Option	Description
<b>Enable communications between clients and the management server</b>	Ensures that the management server and the client computers in this location stay connected, even if the connection for the group is disabled. <b>Note:</b> If <b>Use Group Communication Settings</b> is unchecked for a location, then this option appears for that specific location.
<b>Management Server List</b>	Specifies the management servers that the clients in the group can connect to. Servers that you previously added from the management server list in the Policy Components pane appear in this drop-down list. You can apply one management server list at a time.
<b>Download</b>	Downloads the policies from any server in the management server list by using one of the following methods: <ul style="list-style-type: none"><li>• <b>Download policies and content from the management server</b> Group-specific setting only.</li><li>• <b>Push mode</b> The client establishes a constant connection to the server. Whenever a change occurs with the server status, it notifies the client immediately.</li><li>• <b>Pull mode</b> The client connects to the server periodically, depending on the frequency of the heartbeat setting. The client checks the status of the server when it connects. Because of the constant connection, push mode requires a large network bandwidth. Most of the time you can set up clients in pull mode.</li></ul>
<b>Upload</b>	<b>Learn applications that run on the client computers</b> The client collects information about the applications that run on the client and sends the data to the management server. You can search for and view information about the applications by using the query tool on any one of the policy panes. <b>Note:</b> To enable this setting, you must also enable site-wide application learning. <b>Note:</b> <a href="#">Site Properties: General</a>



Option	Description
<b>Heartbeat Interval</b>	<p><b>Heartbeat interval</b></p> <p>The frequency with which the client communicates with and retrieves settings from the server. At each heartbeat, the server takes the following actions:</p> <ul style="list-style-type: none"> <li>• Updates the logs.</li> <li>• Updates the security policy.</li> <li>• Checks the communication status between the client and the server.</li> </ul> <p>The default heartbeat interval is 5 minutes.</p> <p><b>Let clients upload critical events immediately</b></p> <p>(Windows only) When this option is enabled, the client uploads critical events to the management server immediately and does not wait for the heartbeat interval. Critical events include any risk found (except cookies) and any intrusion event. System change events are not considered critical events. This option is enabled by default.</p> <p>Administrator notifications can alert you right away when the damper period for relevant notifications is set to <b>None</b>.</p> <p><b>Note:</b> Only clients that run version 12.1.4 or later can send critical events immediately. Earlier clients send events at the heartbeat interval only</p> <p>The download mode (push or pull) does not interact with this setting.</p>
<b>Download Randomization</b>	<p><b>Enable randomization</b></p> <p>Configures whether or not the Symantec Endpoint Protection Manager randomizes content downloads from the default management server or a Group Update Provider. Typically, you do not need to change the default settings.</p>
<b>Reconnection Preferences</b>	<p>When you deploy a client installation package, you specify which group the client goes in. You can move the client to a different group. If the client later gets deleted or disconnected and then gets added again and reconnected, the client returns to the original group. Use these settings to keep the client with the group it was last moved to.</p> <ul style="list-style-type: none"> <li>• <b>Use the client's last-used Group setting</b> (Windows and Mac) Use the settings for the group that the client was in before the client disconnected.</li> <li>• <b>Use the client's last-used User mode/Computer mode setting</b> (Windows only) If a new user logs on to a client that is configured in user mode, the client stays in the group that the previous user was in. <a href="#">Switching a Windows client between user mode and computer mode</a></li> </ul> <p>This feature is group-based only, not location-based.</p>

---

## General Settings for group name: General Settings

Use this dialog to configure the general location awareness. These settings are applied to each client within the selected group.

Option	Description
Location Settings	<ul style="list-style-type: none"><li>• <b>Remember the last location</b> At an initial logon, the client is assigned the location that it used last. If location awareness is enabled, the client switches to the appropriate location after a few seconds. If location awareness is disabled, the user can manually switch between any of the locations, even when the client is in server control. If a quarantine location is enabled, the client may change to the quarantine after a short time.</li><li>• <b>Enable Location Awareness</b> Automatically selects the correct location in which to place the clients. The location determines which policy takes effect. Restarts the client in the same location as the location before the user turned off the client computer.</li></ul> <p><b>Note:</b> You can use location awareness only for clients in the subgroups that do not inherit their policy contents from a parent group.</p> <p>These options are enabled by default.</p>
Disable the notification area icon	<p>Use this option for clients that run on a terminal server (such as the Microsoft Terminal Server or Citrix Presentation Server) and that cause high CPU usage and memory usage. Disabling the notification area icon (system tray icon) prevents multiple instances of user session processes (like SmcGui.exe and ccSvcHost.exe) from running.</p> <p>When this feature is enabled, it changes the HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\LaunchSmcGui parameter in the registry to 0. In previous versions, this key would need to be manually changed to 0. The default setting for this feature is disabled, which will toggle that registry key value to 1. As this setting is now managed via policy, any manual changes to this key will be overwritten. Therefore, as a best practice, move clients that are on a terminal server in the same group before you enable this setting. For clients that do not run on terminal servers, keep this option unchecked.</p> <p>This option does not take effect until the smc service is restarted on the client computer.</p> <p>This setting is available as of 14.3 RU1.</p> <p><a href="#">Persistent per-user ccSvcHst.exe processes prevent graceful session logoff</a></p> <p><a href="#">Citrix and terminal server best practices for Endpoint Protection</a></p>

## General Settings for group name: Security Settings

You can configure traffic communication settings on the client.

**Table 319: Security options for clients in a group**

Option	Description
<b>Block all traffic until the firewall starts and after the firewall stops</b>	<p>Blocks all inbound traffic to and outbound traffic from the client computer when the firewall does not run for any reason.</p> <p>The computer is not protected:</p> <ul style="list-style-type: none"> <li>• After the client computer turns on and before the firewall service starts</li> <li>• After the firewall service stops and the client computer stops</li> </ul> <p>This time frame is a small security hole that can allow unauthorized communication. This setting prevents unauthorized applications from communicating with other computers.</p> <p>This option is disabled by default.</p> <p><b>Note:</b> When Network Threat Protection is disabled, the client ignores this setting.</p>
<b>Allow initial DHCP and NetBIOS traffic</b>	<p>Allows the initial traffic that enables network connectivity. This traffic includes the initial DHCP and NetBIOS traffic that allows the client to obtain an IP address. All other traffic is blocked.</p>
<b>Enable secure communications between the management server and clients by using digital certificates for authentication</b>	<p>Enables the clients to authenticate server communication by using certificates. If the certificate is corrupted or invalid, clients cannot communicate with the server. If this option is disabled and the certificate is corrupted or invalid, then the clients can still communicate with the server.</p>

## Password Settings

To provide additional security on the client, you can add password protection for Windows clients based on their group. You can also require a password for uninstalling the Mac client.

**Table 320: Password options for clients in a group**

Option	Description
<b>Require a password to open the client user interface</b>	<p>Users must type a password to open the client from the Windows Start menu or from the notification area icon.</p>
<b>Require a password to stop the client service</b>	<p>Users must type a password to stop the client service. This requirement applies when the user types <code>smc -stop</code> at the command-line prompt. After you type the correct password, it disables the client service and all its technologies within one minute (as of 14.3). If you type an incorrect password, the client is not disabled.</p>
<b>Require a password to uninstall the client</b>	<p>Users must type a password when they uninstall the Windows client.</p>
<b>Require a password to import or export a policy and to import client communication settings</b>	<p>Users must type a password to import, export, and download a new policy, and to import client communication settings.</p>
<b>Apply password settings to non-inherited subgroups</b>	<p>Propagates the password settings in the <b>Client Password Protection</b> group box to subgroups, even when those subgroups do not inherit from the parent group.</p> <p>This option only appears on the parent group.</p> <p><a href="#">Disabling a group's inheritance</a></p>

[Windows commands for the Endpoint Protection client service](#)

## Client User Interface Control Settings for <group name>

You can determine which protection features and client user interface settings are available for users to configure on the client. To determine which settings are available, you specify the user control level. The user control level determines whether the client can be completely invisible, display a partial set of features, or display a full user interface.

### NOTE

For the Windows client, you can configure all the options. For the Mac client, only the notification area icon and some IPS options are available in server control and client control.

The end user must be in a Windows administrators group to change any of the settings in client mode or mixed mode.

**Table 321: Control settings for user control levels**

Option	Description
<b>Server control</b>	<p>Gives the users the least control over the client. Server control locks the managed settings so that users cannot configure them. These settings appear dimmed or unavailable.</p> <p><b>Server control has the following characteristics:</b></p> <ul style="list-style-type: none"><li>• Users cannot configure or enable firewall rules, application-specific settings, firewall settings, and intrusion prevention settings. You configure all the firewall rules and security settings that appear on the client in the console.</li><li>• Users can view the Network and Host Exploit Mitigation logs, Client Management logs, the client's traffic activity, and the list of applications that the client runs.</li><li>• You can configure certain user interface settings and intrusion prevention notifications to appear or not appear on the client. For example, you can hide the client user interface.</li></ul> <p>When you create a new location, the location is automatically set to Server control.</p>
<b>Client control</b>	<p>Gives the users the most control over the client. Client control unlocks the managed settings so that users can configure them.</p> <p><b>Client control has the following characteristics:</b></p> <ul style="list-style-type: none"><li>• Users can configure or enable firewall rules, firewall settings, application-specific settings, intrusion prevention settings, and client user interface settings.</li><li>• The client ignores the firewall rules that you configure for the client.</li></ul> <p>Client control is useful for employees who work in a remote location or a home location.</p>
<b>Mixed control</b>	<p>Gives the user a mixture of control over the client.</p> <p><b>Mixed control has the following characteristics:</b></p> <ul style="list-style-type: none"><li>• Users can configure the firewall rules and application-specific settings.</li><li>• You can configure the firewall rules, which may or may not override the rules that users configure. The position of the server rules in the Rules list of the firewall policy determines whether server rules override client rules.</li><li>• You can configure Network and Host Exploit Mitigation logs, Client Management logs, firewall settings, intrusion prevention settings, and some user interface settings to appear on the client so that users can enable and disable them. The settings that you set to <b>Client</b> are available for the user to configure. The settings that you set to Server are available for you to configure and either appear dimmed or are not visible in the client user interface.</li><li>• You can configure virus and spyware settings to override the setting on the client, even if the setting is unlocked.</li></ul> <p>For example, if you unlock the Auto-Protect feature and the user disables it, you can enable Auto-Protect.</p> <p><b>Note:</b> For the Mac client, you can configure the override settings for the Auto-Protect options only.</p>

---

## Client User Interface Mixed Control Settings: Client/Server Control Settings

Use this dialog box to determine which features are available on the client for the user to configure. These settings apply for the location and not the group.

**You can set managed client user interface settings and Network and Host Exploit Mitigation settings to server control (lock) or client control (unlock) by using the following criteria:**

- If you click **Server**, the setting is not visible or is dimmed on the client. The user cannot configure or enable this feature. Instead, you can configure the setting in another location in the console. This action is also called locking the feature.
- If you click **Client**, the setting is visible on the client. The user can configure or enable the setting. This action is also called unlocking the feature.

You do not lock Virus and Spyware Protection or Memory Exploit Mitigation settings on this tab. You lock and unlock these settings in their associated panes in their policies.

Instead, the Virus and Spyware Protection policy server settings override the client settings by using the following criteria:

- If you click **Server**, the server overrides the client setting, even if the setting is unlocked on the client.
- If you click **Client**, the server setting does not override the client setting.

### NOTE

You can configure all mixed mode options for the Windows client. For the Mac client, you can override the options with an asterisk (\*) in server control and client control.

\*\* The **Client User Interface Settings** tab is on the same dialog box as this tab.

[Client user interface and client logging options](#) describes the client user interface settings that you can lock or unlock and where these options are located on the console and on the client.

**Table 322: Client user interface and client logging options**

Option	Location where you configure this setting
<b>Auto-Protect options*</b>	Windows client: <b>Change Settings &gt; Virus and Spyware Protection &gt; Configure Settings &gt; Auto-Protect tab</b> Mac client: <b>Settings &gt; Virus and Spyware Protection &gt; Auto-Protect Settings &gt; Configure</b>
<b>SONAR protection options</b>	Windows client: <b>Change Settings &gt; Proactive Threat Protection &gt; Configure Settings &gt; SONAR tab</b>
<b>Quarantine options</b>	<b>View Quarantine</b>
<b>Miscellaneous options</b> Miscellaneous options include the Internet Browser Protection settings	Windows client: <b>Change Settings &gt; Virus and Spyware Protection &gt; Configure Settings &gt; Global Settings tab</b>
<b>Show/Hide notification area icon</b> Displays or hides the notification area icon and its right-click menu. The user can still access the client's main window from the Windows Start menu.	<ul style="list-style-type: none"><li>• Console: <b>Client User Interface Settings tab** &gt; Display the notification area icon</b></li><li>• Client: <b>Change Settings &gt; Client Management &gt; Configure Settings &gt; General tab &gt; Show Symantec security icon in notification area</b></li></ul>

Option	Location where you configure this setting
<b>Configure the Control, Packet, Traffic, System, and Security logs</b> Displays the Logs tab, where the user can configure the log size, number of days the log entries are saved, and enables the Packet log.	<ul style="list-style-type: none"> <li>Console  <b>Clients</b> page &gt; <b>Policies</b> tab &gt; <b>Client Log Settings</b> dialog box  <a href="#">Specifying client log size and which logs to upload to the management server</a> </li> <li>Client  <b>Change Settings</b> &gt; <b>Network and Host Exploit Mitigation</b> &gt; <b>Configure Settings</b> &gt; <b>Logs</b> tab </li> </ul>

[Network Threat Protection settings](#) describes the general settings that you can lock or unlock and where these options are located on the console and on the client. Network Threat Protection includes the firewall and intrusion prevention.

**Table 323: Network Threat Protection settings**

Option	Description	Location where you configure this setting
<b>Block all traffic menu command</b>	Blocks all network traffic. If users do not use this command, the client takes action on the traffic that is defined in the firewall rules.	<ul style="list-style-type: none"> <li>Console None</li> <li>Client  <b>Status</b> &gt; <b>Network and Host Mitigation</b> &gt; <b>Options</b> &gt; <b>View Network Activity</b> &gt; <b>Tools</b> menu &gt; <b>Block All Traffic</b> </li> </ul> <p><b>Note:</b> This option appears for users in mixed control on a managed client only, and not an unmanaged client. Users can use this setting but cannot configure it.</p>
<b>Block all traffic until the firewall starts and after firewall stops</b>	Blocks the computer from receiving traffic between the time that the client service starts and the firewall starts. The client also blocks traffic between the time that the firewall shuts down and the client service shuts down.	<ul style="list-style-type: none"> <li>Console  <b>Clients</b> page &gt; <b>Policies</b> tab &gt; <b>General Settings</b> &gt; <b>Security Settings</b> tab </li> <li>Client  <b>Change Settings</b> &gt; <b>Network and Host Exploit Mitigation</b> &gt; <b>Configure Settings</b> &gt; <b>Firewall</b> tab </li> </ul>
<b>Enable/Disable Network Threat Protection</b>	Enables and disables the firewall and the intrusion prevention system. When you disable Network Threat Protection, the client allows all inbound traffic and outbound traffic. You can disable Network Threat Protection from the console at any time using the command on the <b>Clients</b> page. If you run the disable command on the console, it overrides this setting <a href="#">Running commands on client computers from the console</a>	<ul style="list-style-type: none"> <li>Console  <b>Client User Interface Settings</b> tab** &gt; <b>Allow the following users to enable and disable the firewall</b> </li> <li>Client  <b>Status</b> &gt; <b>Network and Host Exploit Mitigation</b> &gt; <b>Options</b> &gt; <b>Enable Network Threat Protection</b> or <b>Disable all Network Threat Protection features</b> </li> </ul>
<b>Test Network Security menu command</b>	Lets the users test the effectiveness of the client computer to outside network threats and viruses by scanning it. The Test Network Security menu command opens the Symantec Security Check website.	<ul style="list-style-type: none"> <li>Console  <b>Client User Interface Settings</b> tab** &gt; <b>Allow users to perform security test</b> </li> <li>Client  <b>Status</b> &gt; <b>Network and Host Exploit Mitigation</b> &gt; <b>Options</b> &gt; <b>View Network Activity</b> &gt; <b>Tools</b> &gt; <b>Test Network Security</b> menu command </li> </ul>

Option	Description	Location where you configure this setting
<b>Configure unmatched IP traffic settings</b>	Controls the incoming IP traffic and outgoing IP traffic that does not match any firewall rules. IP traffic includes the data packets that flow through IP networks and that use the TCP, UDP, and ICMP protocols. Applications, mail exchanges, file transfers, ping programs, and web transmissions are types of IP traffic.	<ul style="list-style-type: none"> <li>Console <b>Client User Interface Settings</b> tab** &gt; <b>Unmatched IP Traffic Settings</b> group box (mixed control only)</li> <li>Client <b>Change Settings &gt; Network and Host Exploit Mitigation &gt; Configure Settings &gt; Firewall</b> tab</li> </ul>

[Firewall policy settings](#) describes the settings that you can lock or unlock. If you set an option to Server, you must also enable or disable it in the Firewall policy.

**Table 324: Firewall policy settings**

Option	Description	Location where you configure this setting
<b>Built-in Rules</b>	Firewall rules that allow the outbound requests and inbound replies for the specified traffic. <a href="#">Built-in Rules</a>	<ul style="list-style-type: none"> <li>Console Firewall policy &gt; <b>Built-in Rules</b></li> <li>Client <b>Change Settings &gt; Network and Host Exploit Mitigation &gt; Configure Settings &gt; Firewall</b> tab</li> </ul>
<b>Protection and Stealth Settings</b>	Firewall rules that allow or block certain types of inbound and outbound traffic. <a href="#">Protection and Stealth Settings</a>	<ul style="list-style-type: none"> <li>Console Firewall policy &gt; <b>Protection and Stealth</b></li> <li>Client <b>Change Settings &gt; Network and Host Exploit Mitigation &gt; Configure Settings &gt; Firewall</b> tab</li> </ul>
<b>Enable network application monitoring</b>	Lets you monitor the applications in use.	<ul style="list-style-type: none"> <li>Console <b>Clients</b> page** &gt; <b>Policies</b> tab &gt; <b>Location-independent Policies and Settings &gt; Network Application Monitoring</b></li> <li>Client <b>Change Settings &gt; Network and Host Exploit Mitigation &gt; Configure Settings &gt; Firewall</b> tab</li> </ul>

[Enabling communications for network services instead of adding a rule](#)

[Intrusion Prevention policy](#) describes the intrusion prevention settings that you can lock or unlock and where these options are located on the console and on the client.

**Table 325: Intrusion Prevention policy**

Option	Description	Location where you configure this setting
<b>Enable Intrusion Prevention</b>	Applies network IPS signatures, exceptions to IPS signatures, and IPS custom signatures to inbound and outbound traffic on the client.	<ul style="list-style-type: none"> <li>Console Intrusion Prevention policy &gt; <b>Intrusion Prevention</b></li> <li>Client <b>Change Settings &gt; Network and Host Exploit Mitigation &gt; Configure Settings &gt; Intrusion Prevention</b> tab</li> </ul>
<b>Enable Browser Intrusion Prevention</b>	Applies IPS web browser signatures to inbound and outbound browser traffic on the client.	<ul style="list-style-type: none"> <li>Console Intrusion Prevention policy &gt; <b>Intrusion Prevention</b></li> <li>Client <b>Change Settings &gt; Network and Host Exploit Mitigation &gt; Configure Settings &gt; Intrusion Prevention</b> tab</li> </ul>
<b>Show/Hide Intrusion Prevention notifications</b>	Displays the notifications that appear when an intrusion prevention attack is launched against the client computer. You can configure the notifications to occur with a sound or to close after a certain period of time. You can also configure firewall notifications.	<ul style="list-style-type: none"> <li>Console <b>Client User Interface Settings</b> tab** &gt; <b>Network Protection Security Event Notification</b> group box</li> <li>Client <b>Change Settings &gt; Network and Host Exploit Mitigation &gt; Configure Settings &gt; Notifications</b> tab</li> </ul>

**Table 326: Web and Cloud Access Protection policy**

Option	Description	Location where you configure this setting
<b>Enable Web and Cloud Access Protection</b>	Redirects traffic using Web Security Service (WSS) technologies.	<ul style="list-style-type: none"> <li>Console Web and Cloud Access Protection policy &gt; <b>Web and Cloud Access Protection</b></li> <li>Client <b>Change Settings &gt; Client Management Settings &gt; Configure Settings &gt; WSS Traffic Redirection</b> tab If this feature is set to client control, the user can only enable or disable it. The user cannot change the Proxy Auto Configuration (PAC) file location. <b>Note:</b> This feature is not supported for the Mac client.</li> </ul>

[Enabling network intrusion prevention or browser intrusion prevention](#)

## Client User Interface Settings

You can configure general user interface settings and some protection settings for the client. These settings apply to the selected location.

You can configure these settings if:

- You had set the client's user control level to server control.
- You had set the client's user control level to mixed control and set the parent feature on the **Client/Server Control Settings** tab to **Server**.

For example, if you set **Show/Hide notification area icon** to **Server**, you choose whether to show or hide the icon on the client. If you set **Show/Hide notification area icon** to **Client**, the user on the client sees the notification area icon. The user can then choose to show or hide the icon.



## NOTE

For the Windows client, you can configure all the options. For the Mac client, you can configure the options with an asterisk (\*) in server control and client control.

**Table 327: Client user interface features**

Option	Description	Location where you configure this setting
<b>Display the client</b>	Displays the client user interface. If the user interface is hidden, the client runs in the background.	Console: <b>Client/Server Control Settings</b> tab (server control only) Client: <ul style="list-style-type: none"><li>In server control, if you uncheck this option, the notification area icon does not appear on the client, even if the <b>Display the notification area icon</b> option is checked.</li><li>In mixed control, you cannot disable the <b>Display the client</b> option. Users can still open the client's main window from the <b>Start</b> menu.</li></ul>
<b>Display the notification area icon*</b>	Displays the client's notification area icon and its right-click menu.	<ul style="list-style-type: none"><li>Console: <b>Client/Server Control Settings</b> tab &gt; <b>Show/Hide notification area icon</b></li><li>Client: <b>Change Settings &gt; Client Management &gt; Configure Settings &gt; General</b> tab &gt; <b>Show Symantec security icon in notification area</b></li></ul>
<b>Enable Windows toast notifications</b>	Shows or hides pop-up notifications on the Windows 8 style user interface.	<ul style="list-style-type: none"><li>Console <b>Client/Server Control Settings</b> tab (Server control only)</li><li>Client: <b>Change Settings &gt; Client Management &gt; Configure Settings &gt; General</b> tab &gt; <b>Use Windows toast for critical alerts</b> In mixed control, you cannot disable the option, and users always see it.</li></ul>
<b>Allow users to perform security test</b>	Displays the <b>Test Network Security</b> menu command in the Network and Host Exploit Mitigation module. This menu command opens the Symantec Security Check website. You or the user can run the scans on the site to test the effectiveness of the client against network attacks and viruses. You can use the results of these tests to more effectively configure protection for the client computer.	<ul style="list-style-type: none"><li>Console: <b>Client/User Interface Settings</b> tab &gt; <b>Test Network Security menu command</b></li><li>Client: <b>Status &gt; Network and Host Exploit Mitigation &gt; Options &gt; View Network Activity &gt; Tools &gt; Test Network Security</b></li></ul>

Option	Description	Location where you configure this setting
<b>Allow the following users to enable and disable the firewall</b>	<ul style="list-style-type: none"> <li>• <b>Windows administrators only</b> or <b>All users</b> Specifies which types of users can enable or disable the firewall on the client.</li> <li>• <b>When the firewall is disabled</b> When Network Threat Protection is disabled, the firewall and the intrusion prevention system can ignore all traffic or only inbound traffic. <ul style="list-style-type: none"> <li>– <b>Allow all traffic</b> Disables Network Threat Protection so that both inbound traffic and outbound traffic can pass through the firewall unrestricted.</li> <li>– <b>Allow all outbound traffic only</b> Disables Network Threat Protection for outbound traffic only so that users can access the network. Inbound traffic must still pass through the firewall and the IPS. You might use this option when users connect to the corporate network from a hotel or hot spot. For example, when employees use their corporate laptops away from the office, they can only connect to external websites through their corporate VPN. However, employees may need to first enter information on an external webpage before they can start their VPN. This option allows employees to access the webpage but block inbound traffic.</li> </ul> </li> </ul>	Console: <b>Client/Server Control Settings</b> tab > <b>Enable/Disable Network Threat Protection</b> Client: <b>Disable all Network Threat Protection features/Enable Network Threat Protection</b>
<b>Amount of time before re-enabling Network Threat Protection</b> <b>Number of times users are permitted to disable Network Threat Protection</b>	You can also block users from disabling the protection for more than five minutes or for more than three times. These options ensure that security is restored after employees log on to the webpage.	None
<b>Allow user to enable and disable the application device control</b>	In rare cases, application control might interfere with some safe applications that run on client computers. You might want to allow users to disable this option to troubleshoot problems.	Console: Application and Device Control policy > <b>Enable this policy</b> Client: <b>Change Settings &gt; Client Management &gt; Configure Settings &gt; General tab &gt; Enable Application and Device control</b>

Option	Description	Location where you configure this setting
<b>Network Protection Security Event Notification</b>	<ul style="list-style-type: none"> <li>• <b>Display Intrusion Prevention and Memory Exploit Mitigation notifications*</b> Displays the notifications every time the IPS detects an intrusion prevention attempt or if MEM detects an exploit. If the client detects a second attack when a previous notification is displayed, users see one notification only.</li> <li>• <b>Use sound when notifying users*</b> User hears a sound when a notification appears.</li> <li>• <b>Additional text for notifications*</b> To avoid the truncation of the notification text, you should limit your added text to no more than 120 characters. (For Mac, Server control only)</li> </ul>	Console <b>Client/Server Control Settings</b> tab > <b>Show/Hide Intrusion Prevention notifications</b> Client: <b>Change Settings &gt; Network and Host Exploit Mitigation &gt; Configure Settings &gt; Notifications</b> tab > <b>Display Intrusion Prevention and Memory Exploit Mitigation notifications</b> and <b>Use sound when notifying users</b>
<b>Unmatched IP Traffic Settings</b> (Mixed control only)	Controls the incoming IP traffic and outgoing IP traffic that does not match any firewall rules. IP traffic includes the data packets that flow through IP networks and that use the TCP, UDP, and ICMP protocols. Applications, mail exchanges, file transfers, ping programs, and web transmissions are types of IP traffic. <ul style="list-style-type: none"> <li>• <b>Allow IP traffic</b> Allows any incoming traffic and outgoing traffic, unless a firewall rule states otherwise. For example, if you add a firewall rule that blocks VPN traffic, the firewall allows all other traffic except for the VPN traffic. If you uncheck this option, the firewall is disabled.</li> <li>• <b>Allow only application traffic</b> Allows the traffic to and from applications and blocks the traffic that is not associated with any application. For example, the firewall allows Internet Explorer but blocks VPN traffic, unless a firewall rule states otherwise.</li> <li>• <b>Prompt users before allowing application traffic</b> Displays a message that asks the user whether to allow or block an application. For example, users can choose whether or not to block media files. Or, users can hide broadcasts from the NTOSKRNL.DLL process. The NTOSKRNL.DLL process can be an indication of spyware, because spyware often downloads and installs the NTOSKRNL.DLL process.</li> </ul>	Console: <b>Client/Server Control Settings</b> tab > <b>Configure unmatched IP settings</b> Client: <b>Change Settings &gt; Network and Host Exploit Mitigation &gt; Configure Settings &gt; Firewall</b> tab

## Specify Location Criteria

You can specify a number of conditions to determine when a client computer is allowed to switch to another location before connecting to the network. Switching locations lets you apply a different set of security policies when a client computer connects from a more vulnerable location. If the conditions match, the computer automatically switches to the designated group's location with its associated policy and the computer is allowed to connect to the network.

The conditions that you set may be positive. For example, a client computer matches because it uses an IP address within a specified IP address range or it has a particular registry key. Conditions can also be negative. For example, a computer matches if it does not use a specific Wireless SSID that you have specified.

#### NOTE

The following conditions work with the Client Update policy (14.3 RU3 and later): Host Name, User or Group Name, File Exists, and Operating System.

**Table 328: Location criteria**

Option	Description
Computer IP Address	You can specify the following types of device IP address conditions: IP Address, IP Range, Subnet Address, or Host Group and their values. IPv4 or IPv6 is supported for IP Address, IP Range, or Subnet Address. With <b>Host group</b> as the Address Type, the target rule ignores any DNS host, DNS domain, or MAC address configured for the host group. The rule only honors host groups configured with IP address, IP address range, or IP subnet.
Gateway Address	This condition matches on the Gateway IP address. A default gateway is an IP address that traffic gets sent to when it's bound for a destination outside the current network. You can specify the following criterion types: IP Address, IP Range, Subnet Address, Host Group, or a MAC Address and their values. You can also specify IPv4 or IPv6 for IP Address, IP Range, or Subnet Address.
WINS Server Address	This condition matches on the WNS server address. You can specify the following criterion types: IP Address, IP Range, Subnet Address, or Host Group and their values. You can also specify IPv4 or IPv6 for IP Address, IP Range, or Subnet Address.
DNS Server Address	This condition matches on the DNS server address. You can specify the following criterion types: IP Address, IP Range, Subnet Address, or Host Group and their values. You can also specify IPv4 or IPv6 for IP Address, IP Range, or Subnet Address.
DHCP Server Address	This condition matches on the DHCP server address. You can specify the following criterion types: IP Address, IP Range, Subnet Address, Host Group, or a MAC Address and their values. You can also specify IPv4 or IPv6 for IP Address, IP Range, or Subnet Address.
Network Connection Type	This condition matches on the network connection type, such as a Cisco VPN.
Management Server Connection	This condition matches when a device is connected or not connected to the specified Symantec Endpoint Protection Manager.
Trusted Platform Module	You can specify the following Trusted Platform Module (TPM) types: <ul style="list-style-type: none"> <li>Any TPM Token</li> <li>IBM TPM Token</li> <li>HP TPM Token</li> </ul>
DNS Lookup	This condition matches when a device resolves or does not resolve the specified host name and IP type.
Registry Key	This condition matches when the device's registry has a setting that is equal or not equal to the specified registry key, registry key name, or registry value.
Wireless SSID	This condition matches if the device uses or does not use any of the specified SSIDs.
NIC Description	This condition matches when a device has a Network Interface Card (NIC) that matches or does not match the description.
DHCP Connection DNS Suffix	This condition matches when the device uses or does not use the specified DNS suffixes.
ICMP Request (Ping)	You can specify the following types of ICMP request conditions: IP Address, Host Name, or Host Group and their values. IPv4 or IPv6 is supported for IP Address.
Host Name*	This condition matches on the computer's host name. You can use the wildcards asterisk (*) and question mark (?). Depending on your network setup, you may need to use the full DNS name. For example: <i>somehost*.companyname.com</i> .

Option	Description
User or Group Name*	This condition matches on the user name or the group name, such as <code>admin</code> or <code>My Company</code> . You can use the wildcards asterisk (*) and question mark (?). However, you might find that a user unexpectedly triggers the rule because of the user name or group name. For example: You define a condition as <code>contains Adminis*</code> . You might expect that only user names starting with <code>Adminis</code> trigger the rule. But any domain user name triggers the rule because the domain administrator group name matches the condition.
File Exists*	This condition checks that a certain file exists on the specified path on the client. For example, you can use this condition to find computers that run a text file that upgrades the clients.
Operating System*	This condition matches on a particular operating system, based on the version number, build number, and architecture (such as 32-bit or 64-bit computers). For example, you may want to automatically upgrade computers with older client installation packages, regardless of which group they are in.

\*You can use this condition in the Client Upgrade policy (14.3 RU3 or later).

## Address

In the Address dialog box, you can specify the location switching conditions that are based on the following criteria:

- An IP address
- An IP range
- A subnet address
- A host group
- A MAC address

**Table 329: Switching options based on IP addresses, host names, and host groups**

Option	Description
<b>IP Address</b>	Specifies the IP address that you want to match for this location criterion. Both IPv4 and IPv6 are supported.
<b>IP Range</b>	Specifies the starting IP address and the ending IP address of the range of addresses that you want to match for this location criterion. Both IPv4 and IPv6 are supported.
<b>Subnet Address</b>	Specifies the subnet and the subnet mask that you want to match for this location criterion. Both IPv4 and IPv6 are supported.
<b>Host Group</b>	Specifies the criteria that determines which location host groups can switch to and lets you specify the group name that is linked to the criteria.
<b>MAC Address</b>	Specifies the MAC address that you want to match for this location criterion.

[Specify Location Criteria](#)

[Adding a location to a group](#)

## Manage Locations

You can manage the locations and network connection types client computers can use to connect to the internal network. To manage these, use the following location-specific settings in the **Manage Locations** dialog box.

**Table 330: Manage Locations**

Field	Description
Locations	Contains a list of locations that have been added for a group.
Enable this location	When this option is checked, it causes the location to be immediately enabled.
Set this location as the default location in case of conflict	When this option is checked, it makes this location the default location.
Switch to this location when	Contains a list of conditions that must be met before the client can switch to another location.
DNS Query Loop in	<p>When this option is checked and the number of seconds specified, queries the DNS server at the specified interval. You can define how frequently you want a specific location to perform a DNS query. This feature lets you configure one location to query the DNS server more often than other locations. For example, assume that you have a policy to block all traffic outside of your corporate network except VPN traffic. And assume that your users travel and must access your network through a VPN from a hotel network. You can create a policy for a VPN connection that uses DNS resolution. Symantec Endpoint Protection continues to send the DNS query every 5 seconds until it switches to this location. This way, your users can more quickly access your network. The default value is 30 minutes.</p> <p>Use caution when you configure this setting to a very low value. You run the possibility of bringing down your DNS server if all of your systems access the server every 5 seconds, for example.</p>
ICMP Request Loop in	When this option is checked and the number of seconds specified, checks for ICMP ping requests at the specified interval.
The location will be checked every	The time interval after which the location is checked.
Enable location change notification	When this option is checked, it enables an email notification when a location change occurs.

**NOTE**

[Enabling location awareness for a client](#)

[Adding a location to a group](#)

## Select Restart Options

[Restart settings](#) provides explanations to help you understand which options to use in various situations.

**NOTE**

These settings only apply to Windows client computers. Mac client computers always perform a hard restart. The Linux clients do not restart by a restart command from the management server.

Table 331: Restart settings

Setting	Description
Restart method	<ul style="list-style-type: none"> <li>• <b>Forced restart</b> Use this option when the need to restart the computer is more important than the effect on the user. The user cannot delay the restart of their computer. This option is valuable when you mitigate a threat or preminent attack.</li> <li>• <b>Delayed restart</b> You can delay the client restart by an interval you select. Often you delay a restart to accommodate the needs of the user. You can allow the user to postpone when the computer restarts. The user is given five minutes to save any unsaved data.</li> <li>• <b>No restart</b> Use this option if there is no immediate threat or need to restart the client computer at a particular time. This option is a good choice when you can safely wait to restart the computer as part of the normal user routine. In some cases, you may be required to restart the client computer to start a service. You receive a notification when this requirement is present.</li> <li>• <b>Custom restart</b> Use this option when you need a combination of settings that the other restart methods do not provide.</li> </ul>
Restart client computer	<ul style="list-style-type: none"> <li>• <b>Immediately</b> Use this option when you must restart the client computer without delay. Situations that may require an immediate restart include malware remediation, schedule urgency, and proactive protection against an imminent threat. Use with <b>Forced Restart</b> for the most rapid computer restarts.</li> <li>• <b>Up to this time:</b> or <b>At this time:</b> Use this option when an immediate restart may affect work, or when you can safely delay the restart. Be sure that you understand the implications of delaying a restart when an active threat is present.</li> <li>• <b>Randomize the start time to be + or - 2 hours</b> Use this option to avoid conflicts with other scheduled tasks and to control client restart behavior. Restart randomization lets the clients restart at different times within a range of one to eight hours. This option is useful in virtualized environments to alleviate hardware overload. This overload can occur when all virtual machines that are hosted on a server restart at the same time.</li> </ul>
Prompt	<ul style="list-style-type: none"> <li>• <b>No prompt</b> This option is typically used with the <b>At this time</b> option to suppress the restart prompt during times when the user is away from the computer.</li> <li>• <b>Prompt with a countdown of</b> Use this option to display a prompt informing the user that a restart is imminent. This option is especially useful when used with the settings <b>Immediately</b> and <b>At this time</b>.</li> <li>• <b>Prompt and allow user to delay restart until</b> Use this option when you must restart the client computer within a given period of time. This option gives the user a chance to save data and exit programs, and ensures that they restart the computer.</li> </ul>
Restart Message	The message that appears in the prompt informs the user that the computer is about to restart.
Other options	<p>These options control the behavior of the client computer as it relates to other programs that may be running at the time of the restart.</p> <p>These options apply only to Windows clients. Mac clients always perform a hard restart.</p> <ul style="list-style-type: none"> <li>• <b>Hard restart</b> This option forces the client computer to restart regardless of any other activity occurring on the client computer. In most cases, this option is not used except in extreme circumstances.</li> <li>• <b>Restart immediately if the user is not logged in</b> If the user is not logged in when the restart request is sent, this option forces an immediate restart and overrides other pending restart actions.</li> </ul>

---

## Cloud Settings

This tab appears after you enroll Symantec Endpoint Protection Manager with the cloud and apply a policy to enable low-bandwidth mode.

**Table 332: The Cloud Settings tab**

Value	Description
<b>Run in low-bandwidth mode</b>	Indicates whether the cloud console's Low Bandwidth policy enables low-bandwidth mode. Since the cloud console creates and controls this policy, you cannot check or uncheck this option from Symantec Endpoint Protection Manager. If the group is running in low-bandwidth mode, ensure that you have enabled <b>Advanced Machine Learning</b> content. <a href="#">Reverting to an older version of the Symantec Endpoint Protection security updates</a>

## Client Submissions

Clients automatically submit pseudonymous information about detected threats as well as network and configuration information to Symantec. Symantec uses this information to address new and changing threats and improve the security features in Symantec Endpoint Protection.

If your organization is part of a Symantec-sponsored custom analysis program, you can choose to send client-identifiable information as well. Symantec can use client-identifiable information to provide customized solutions for your particular environment.

Check the Client Activity log to view the types of submissions that your client computers send and to monitor bandwidth usage. [Viewing logs](#)

[Understanding server data collection and client submissions and their importance to the security of your network](#)



**Table 333: Client Submission settings**

Option	Description
<b>Client submissions</b>	<ul style="list-style-type: none"> <li>• <b>Send pseudonymous data to Symantec to receive enhanced threat protection intelligence</b> Enabled by default. Enables the client computers to submit pseudonymous information to Symantec. Symantec recommends that clients submit information to help Symantec provide improved security. You may need however, to disable this feature in response to network bandwidth issues or a restriction on the data that client computers can send.</li> <li>• <b>More Options</b> You can enable or disable specific types of submissions. The types include file reputation data, process data, network data, and configuration data.</li> <li>• <b>Send client-identifiable data to Symantec for custom analysis</b> Disabled by default Select this option only if you participate in a Symantec-sponsored program to get recommendations specific to your security network.</li> </ul> <p><b>Note:</b> If Symantec Endpoint Protection Manager is enrolled in the cloud, these settings get automatically turned on. The cloud console needs the data to do a better job of threat analysis. You can disable these settings, but Symantec recommends you leave them checked.</p>
<b>Client Queries</b>	<p><b>Allow Insight lookups for threat detection</b> Enabled by default Lets Symantec Endpoint Protection use Symantec's reputation database and extended virus and spyware definitions in the cloud to make decisions about threats. The reputation database is called Symantec Insight. Queries to the database are called Insight lookups or cloud lookups.</p> <ul style="list-style-type: none"> <li>• Starting in 14, Auto-Protect, administrator and on-demand scans, Download Insight, SONAR, and Power Eraser use Insight lookups for threat detection.</li> <li>• On legacy 12.1.x clients, Download Insight, Insight Lookup, SONAR, and Power Eraser use Insight lookups for threat detection.</li> </ul> <p>Symantec recommends that you allow Insight lookups. Disabling Insight lookups disables protection from the cloud. The standard and the embedded client run only the latest definitions locally and require Insight lookups to get the extended set of definitions. Without Insight, Power Eraser makes fewer detections, and the detections are more likely to be false positives. Insight lookups in the cloud are critical to complete protection on your endpoints.</p> <p>You can disable this option if you determine that you do not want to allow Symantec to query Symantec Insight. For example, your company may require you to turn off external communications with the network so that data never leaves the client. If that is the case, you should use the dark network client installation, which includes the full set of definitions.</p>

## Tamper Protection

Tamper Protection protects Symantec processes from non-Symantec processes such as worms, Trojan horses, and viruses. Tamper Protection can block or log the attempts to modify the Symantec processes or the internal software objects that synchronize Symantec threads and processes.

If you use any third-party security risk scanners that detect and defend against unwanted adware and spyware, these scanners typically affect Symantec resources. If you set Tamper Protection to log tamper events when you run such a scanner, Tamper Protection generates a large number of log entries. If you decide to log Tamper Protection events, use log filtering to manage the number of events.

Tamper Protection runs on Windows clients only. It does not run on Mac or Linux clients.

**Table 334: Tamper Protection configuration options**

Option	Description
<b>Protect Symantec security software from being tampered with or shut down</b>	By default, Tamper Protection is enabled.
<b>Actions to take if an application attempts to tamper with or shut down Symantec security software</b>	<ul style="list-style-type: none"> <li>• <b>Log only</b> This action logs the occurrence of unauthorized activity that is directed against Symantec processes.</li> <li>• <b>Block and do not log</b> This action blocks any unauthorized activity that is directed against Symantec processes and but does not log the occurrence of the unauthorized activity.</li> <li>• <b>Block and log</b> This action blocks any unauthorized activity that is directed against Symantec processes and logs the occurrence of the unauthorized activity.</li> </ul> <p>Change the setting to <b>Log only</b> or <b>Block and log</b> if you want to monitor the detections for false positives. Tamper Protection can generate many log messages, so you might not want to log the events.</p>

## Administrators and authentication

### Admin Page: Administrators

Use the Admin page to view general information about the selected administrator.

**Table 335: Admin page settings**

Setting	Options and Descriptions
<b>Administrator Name</b>	The user name of the administrator who is currently logged on.
<b>Full Name</b>	The full name of the administrator.
<b>Email</b>	The administrator's email address to which notifications are sent.
<b>Number of Incorrect Logon Attempts Allowed</b>	The number of times the administrator can try to log on using an invalid password before Symantec Endpoint Protection Manager locks the account.
<b>Online Status</b>	Whether the administrator is online or offline.
<b>Creation Time</b>	The date and the timestamp when the administrator account was created.
<b>Lock Status</b>	The status of the administrator account. The status can be Locked or Not Locked.
<b>Lock Time</b>	The date and the timestamp when the administrator account was locked. If the administrator's account is not locked, this field is empty.
<b>Last Logon IP Address</b>	The most recent IP address to which the selected administrator had logged on.
<b>Last Logon Time</b>	The date and the timestamp when the administrator last logged on.
<b>Last Logout Time</b>	The date and the timestamp when the administrator had last logged out.
<b>Failed Logon Attempts</b>	The number of times that the administrator failed to log on.
<b>Enabled Status</b>	The status for an administrator that you create is Enabled.
<b>Authentication Method</b>	The method that the administrator uses to authenticate on the server.
<b>Number of Change Current Password Attempts Allowed</b>	The number of times you try to change the password on another administrator account, but type an incorrect current password. You get 3 attempts. After 3 attempts, Symantec Endpoint Protection Manager logs you out of the console.

Setting	Options and Descriptions
<b>Failed Change Current Password Attempts</b>	The number of times that you failed to enter the administrator account's current password correctly. This number of attempts resets to 0 after you type the correct current password correctly.
<b>Last Password Change Time</b>	The date and the timestamp of the last time that the administrator password was changed.
<b>Password Expires In</b>	The time period after which the administrator must change the password.
<b>Company Name</b>	For system administrators only. You provide the company name either when you configure the server or when you edit an administrator account.

## Managing administrator accounts

### Change password

Use this dialog box to change an administrator's password.

You must set a strong password for an administrator account. The password must contain at least 8 characters and fewer than 16 characters. It must include at least one lowercase letter [a-z], one uppercase letter [A-Z], one numeric character [0-9], and one special character ["/ \ [ ] : ; | = , + \* ? < > ].

You use the same user name and password for the administrator account as for the default Microsoft SQL Server Express database. The administrator account for the Microsoft SQL Server database has separate requirements.

When you first configured the management server in the Management Server Configuration Wizard, you could select the default installation or custom installation. If you selected the default installation, the password you entered is the same as the encryption password. If you now change the administrator's password, the encryption password does not change.

### Rename Administrator

Use this dialog to change the name of the selected administrator.

**Table 336: Rename Administrator dialog**

Option	Description
New Administrator Name	Renames the selected administrator. The user name must be six to 20 characters in length. The following characters are not allowed: "/ \ [ ] : ;   = , + * ? < > . The new administrator name is updated in the <b>Administrators</b> list.

### Administrator Properties: General

Use this dialog box to add an administrator account, or to edit an existing administrator account.

#### NOTE

The setting for the administrator password never to expire is removed.

**Table 337: Administrator Properties, General tab**

Option	Description
<b>User name</b>	The name that the administrator uses to log on to Symantec Endpoint Protection Manager. The user name must be six to 20 characters in length. The following characters are not allowed: " / \ [ ] : ;   = , + * ? < >
<b>Full name</b>	A full name or the description for the administrator.
<b>Email address</b>	The administrator's email address. If the administrator is locked out of the management server, the administrator receives an email alert at this email address. The management server sends an email message to this email address when the management server locks the administrator's account. You must check the <b>Send an email alert to Administrator when the account is locked</b> check box to send the email message.
<b>Lock the account after the specified number of unsuccessful logon attempts</b>	The number of times that the administrator is unsuccessful in logging on to the management server before the administrator is locked out. You can use this feature to block against the malicious attacks that use random user names and passwords to log on to the management server. If the management server locks out a system administrator, the system administrator is locked out of all domains. If the management server locks out a non-limited and limited administrator, the administrator is locked out of that domain or group only. You can create additional non-limited or limited accounts for the same administrator for different domains. <a href="#">Unlocking an administrator's account after too many logon attempts</a>
<b>Lock the account for the specified number of minutes</b>	The time interval during which the administrator cannot log on to the management server. The default is that this option is checked. Select a time interval between 1 minute and 60 minutes. The default value is 15 minutes. The lockout interval doubles with each subsequent lockout. Symantec Endpoint Protection Manager restores the original lockout interval after a successful logon, or 24 hours after the first failed logon attempt. <b>Note:</b> If an administrator is locked out of their account, they must wait the specified time before logging on again. You cannot unlock an account during the lockout interval. A password change does not unlock a locked account. <a href="#">Unlocking an administrator's account after too many logon attempts</a>
<b>Send an email alert to Administrator when the account is locked</b>	The setting that sends an email message to the administrator when the administrator is locked out of the management server. You must enter a valid email address in the Email address text field.

## Managing administrator accounts

### Administrator properties: Access Rights

Use this tab to specify the administrator account type and access rights as appropriate. For a small company, you may only need one administrator. For a large company with multiple sites and domains, you most likely need multiple administrators, some of whom have more access rights than others.

#### NOTE

Because system administrators have full access rights for all domains, you need to configure access rights for administrators and limited administrators only.

**Table 338: Access rights**

Option	Description
<b>System Administrator</b>	Has full access to all areas of Symantec Endpoint Protection Manager. <b>Note:</b> Only system administrators can administer licenses.
<b>Administrator</b>	Has access rights for most tasks within a single domain, including: <ul style="list-style-type: none"> <li>• Add and manage other domain administrator accounts and limited administrator accounts.</li> <li>• Manage the password rights for limited administrators and other domain administrators with equal or less restrictive site rights.</li> <li>• Manage the database and all servers for a site, by clicking the <b>Site Rights</b> option.</li> </ul>
<b>Limited Administrator</b>	Has access rights for a subset of tasks within one domain, including: <ul style="list-style-type: none"> <li>• <b>View reports:</b> Run and view reports for specific computers.</li> <li>• <b>Manage groups:</b> Manage specific groups. You can enable the administrator to either view and manage the group, view the group only, or hide the group from view.</li> <li>• <b>Remotely run commands:</b> Run specific commands from the console on the client computers. You must check <b>Manage groups</b> to configure this option. <b>Run commands on read-only groups</b> lets a limited administrator run commands on the groups that the limited administrator cannot modify.</li> <li>• <b>Site rights</b> Manage the database and all management servers for a site.</li> <li>• <b>Manage installation packages</b> Manage or view client installation packages.</li> <li>• <b>Manage policies</b> Add and modify both shared and non-shared policies.</li> <li>• <b>Allow editing of shared policies</b> Add and modify non-shared policies only. This checkbox is unselected by default so that you must explicitly grant permissions, instead explicitly denying permissions. In 14.3 RU2, this command was changed from <b>Do not allow editing of shared policies</b>.</li> </ul> <p>The default, limited administrators have full rights over all groups.</p>

## Administrator: Authentication

Use these options to specify the type of authentication that is required for an administrator account. You can specify one of three types of authentication servers.

**Table 339: Authentication options**

Option	Description
<b>Symantec Endpoint Protection Manager Authentication</b>	<p>Authenticates the administrator account by using the Symantec authentication mechanism. You create a user name and password that are stored in the Symantec Endpoint Protection Manager database. When an administrator enters a user name and password to log on to Symantec Endpoint Protection Manager, it is validated against the Symantec Endpoint Protection Manager database.</p> <p><b>Note:</b> You must set a strong password for an administrator account. The password must contain at least 8 characters and fewer than 16 characters. It must include at least one lowercase letter [a-z], one uppercase letter [A-Z], one numeric character [0-9], and one special character such as: ["/ \ [ ] : ;   = , + * ? &lt; &gt; ] @ (14.2 and later)</p> <ul style="list-style-type: none"> <li>• <b>Password never expires</b> Enables the administrators of the domain to use a password that does not expire. To display or hide this option, you configure it in the <b>Passwords</b> tab of the <b>Domain Properties</b> dialog box. <a href="#">Enabling Symantec Endpoint Protection Manager logon passwords to never expire</a></li> <li>• <b>Password will expire in x days</b> Rotates the administrator's password. Symantec recommends that you use this option to increase security against attacks.</li> <li>• <b>Set Password or Change Password</b> Sets a new password for the administrator account for when that administrator logs on to Symantec Endpoint Protection Manager. If you change the administrator's password, you must type your own password first.  <b>Note:</b> A password change does not unlock a locked account. <a href="#">Unlocking an administrator's account after too many logon attempts</a></li> <li>• <b>Enable two-factor authentication using Symantec VIP</b> Two-factor authentication adds an extra layer of security to the logon process. If required, administrators must provide a unique, one-time verification code when they log on, in addition to their password. Turn on this option to require the administrator to use it. They are then prompted to set up two-factor authentication the next time they sign in. This option is available for all Symantec Endpoint Protection Manager administrator types.  <b>Note:</b> Two-factor authentication with Symantec VIP is not supported in FIPS-enabled environments or over IPv6. <a href="#">Configuring two-factor authentication with Symantec VIP</a></li> </ul>
<b>RSA SecurID Authentication</b>	<p>Authenticates the administrator account by using an RSA SecurID server on a separate computer to communicate with the SecurID client. <a href="#">Using RSA SecurID authentication with Symantec Endpoint Protection Manager</a></p>

Option	Description
<b>Directory Authentication</b>	<p>Authenticates the administrator account by connecting to a directory server (either LDAP or Active Directory) and using the account name.</p> <p>You can connect to a directory server in the following ways:</p> <ul style="list-style-type: none"> <li>• <b>Directory Servers</b> option.</li> <li>• The <b>Edit the server properties</b> dialog box on the <b>Admin &gt; Servers</b> page.  <a href="#">Connecting Symantec Endpoint Protection Manager to a directory server</a></li> </ul> <p>After you add a directory server, you select the directory server name and configuration in the <b>Directory Server</b> drop-down list.</p> <p><b>Account Name</b>  The administrator's account name on the directory server. In most cases, entering only the account name allows authentication. If authentication fails, then enter the user principal name, where username is the directory server account name, and domainname is the Active Directory or LDAP domain name: username@domainname</p> <p><b>Check Account</b>  Checks whether the administrator account name exists on the connected Active Directory server or the LDAP server. Symantec Endpoint Protection Manager searches for the account in the directory server.</p> <p><b>Note:</b> So that administrators are never locked out due to a password change on the directory server, create a directory server entry for anonymous access.</p> <p><a href="#">Checking the authentication to a directory server</a></p>
<b>Smart card-based Authentication</b>	<p>Authenticates the administrators who are civilians or military personnel in U.S. Federal Agencies and who must use a PIV card or CAC to log on.</p> <p><a href="#">Configuring Symantec Endpoint Protection Manager to authenticate administrators who log on with smart cards</a></p>

## Group Rights

Use this dialog box to specify what rights the limited administrator has for each group. Expand the **My Company** group to display additional groups.

First choose the access rights for the parent group, and then choose the access rights each child group.

**You can specify the following levels of access for the limited administrator:**

- **Full Access**  
Enables the administrator to view and manage the client computers in the group.
- **No Access**  
Blocks the administrator from being able to see the client computers in the group.
- **Read Only**  
Enables the administrator to view the client computers in the group but not manage them.

## Reporting Rights

Use this dialog box to specify which computers the limited administrator can run reports on. For example, you may want the administrator to run reports on all the employees in a sales group.

You can add the computers by host name or by IP address. Use a comma between each entry.

## Command Rights

You can run commands on the client computer remotely from the console. These commands override the same commands that the users on the client computer run.

---

For example, if the user enables Network Threat Protection on the client computer, you can override that command by selecting the **Disable Network Threat Protection** command.

You can configure each limited administrator to manage different commands. When the limited administrators log on to the server, they can see only the commands that you have given them the rights to see. For example, you can configure LimitedAdministrator1 to run the **Scan** command and **Enable Auto-Protect** command. You can configure LimitedAdministrator2 to run the **Enable Network Threat Protection** command and the **Disable Network Threat Protection** command.

For more information on what these commands do, see:

[What are the commands that you can run on client computers?](#)

## Policy Rights

You can create separate limited administrator accounts to manage each type of policy on the client. When the limited administrators log on to Symantec Endpoint Protection Manager, they can see only the policies and policy-related settings that you have given them the rights to see.

For example, you can enable LimitedAdministrator1 to manage the Firewall policies only and enable LimitedAdministrator2 to manage the LiveUpdate policies only. On the **Policies** page, LimitedAdministrator2 cannot see **Firewall** policy or **Network Application Monitoring** under **Location-independent Policies and Settings**. On the **Policies** page, LimitedAdministrator1 cannot see the **LiveUpdate** policy.

By default, limited administrators can manage all policy types.

## Site Rights

A site includes one or more management servers and one database. You can give administrators no access to a site.

Administrators who are fully authorized to manage a site can modify site rights for other administrators and limited administrators. Administrators who are not authorized to manage a site through **Site Rights** cannot modify site rights for other administrators and limited administrators.

Administrators cannot modify their own site rights. System administrators must perform this function.

**Table 340: Site rights options for administrators**

Option	Description
<b>Select a site</b>	You can select the site that you want to grant or restrict access to from the list.
<b>Not authorized to manage this site</b>	Grants this administrator no access to manage this site.
<b>Authorized to fully manage this site</b>	Grants this administrator full privileges to manage this site.
<b>Custom authorization for managing this site</b> (for limited administrators)	Allows you to configure separate access privileges to the database and the servers in this site.



---

# Domains

## Admin Page: Domains

Use this pane to review detailed information about the selected domain.

[Domains pane](#) includes a list of the selected domain's properties fields and their definitions.

**Table 341: Domains pane**

Row name	Description
Domain Name	The name of the selected domain.
Company	The company name.
Contact List	An optional field that contains the names of domain administrators.
Creation Time	The date and the time stamp of when the selected domain was created.
Enabled Status	The status of the domain can be either Enabled or Disabled.
Number of Administrators	The total number of administrators in the domain.
Domain ID	The unique identifier of the selected domain.

## Add Domain

Use this dialog box to add a new domain. You create a domain to organize a subset of client computers in your organization. For example, you may want to organize users by division. The data in each domain is completely separate, which prevents administrators in one domain from viewing data in other domains. For small businesses, use the default domain only.

**Table 342: Domain options**

Option	Description
<b>Domain Name</b>	The name of the domain. A domain name has a limit of 256 characters, and it cannot be blank. All characters are allowed.
<b>Company Name</b>	The company name.
<b>Contact List</b>	A description field. You can include a list of contacts for the domain, such as the name of the person who is responsible for that site.

Option	Description
<b>Delete clients that have not connected for specified time</b>	<p>Check to delete the clients that do not connect to this domain in the specified number of days. The default is 30 days.</p> <p>Over time, the Symantec Endpoint Protection Manager database may accumulate entries for obsolete clients. Obsolete clients are the clients that no longer function in the environment. Clients can be made obsolete when operating systems are upgraded or when a computer ID is changed. Obsolete clients count against the product license, so it is important to purge obsolete clients quickly. If your license reports show more seats are licensed than known to be deployed, you should purge the database of obsolete clients. You can shorten the purge interval to purge more quickly and then reset the interval to suit your long-term needs after the purge cycle completes.</p> <p><b>Delete non-persistent VDI clients that have not connected for specified time</b></p> <p>In non-persistent Virtual Desktop Infrastructures (VDIs), you can set a separate time period for the non-persistent clients that have not connected. This setting can be equal to but not greater than the time period for all clients. The default is seven days. Use a period that is short enough to make sense in your virtual infrastructure. Symantec does not recommend that you use a long time period.</p> <p>If this setting is not enabled, then non-persistent VDI clients are deleted after the same period of time as all other clients.</p>
<b>Advanced</b>	<p>Lets you set the <b>Domain ID</b>, a unique number that the management server uses to identify the domain. Typically you should leave this field blank. The management server assigns a random ID when you create a new domain.</p> <p>You can use a domain ID for disaster recovery. If all the management servers in your organization fail, you need to rebuild the management server by using the same ID as the old server. You can get the old domain ID from the symlink.xml file on any client.</p>

## Edit Domain Properties: General

Use this tab to change optional information about a domain.

**Table 343: Edit Domain Properties dialog box**

Option	Description
<b>Domain Name</b>	The current domain name. You cannot edit this field.
<b>Company Name</b>	The company name. You can update an existing company name, or can type a new company name if the field is blank. This field is optional and is for informational purposes only.
<b>Contact List</b>	A description field. You can include a list of contacts for the domain, such as the name of the person who is responsible for that site.
<b>Delete clients that have not connected for specified time</b>	<p>Check to delete the clients that do not connect to this domain in the specified number of days.</p> <p>Over time, the Symantec Endpoint Protection Manager database may accumulate entries for obsolete clients. Obsolete clients are the clients that no longer function in the environment. Clients can be made obsolete when operating systems are upgraded or when a computer ID is changed. Obsolete clients count against the product license, so it is important to purge obsolete clients quickly. If your license reports show that more seats are licensed than known to be deployed, you should purge the database of obsolete clients. You can shorten the purge interval to purge more quickly and then reset the interval to suit your long-term needs after the purge cycle completes.</p> <p><b>Delete non-persistent VDI clients that have not connected for specified time</b></p> <p>In non-persistent Virtual Desktop Infrastructures (VDIs), you can set a separate time period for the non-persistent clients that have not connected. This setting can be equal to but not greater than the time period for all clients. The default is 7 days. Use a period that is short enough to make sense in your virtual infrastructure. Symantec does not recommend that you use a long time period.</p> <p>If this option is disabled, then non-persistent VDI clients age the same as all other clients.</p>

Option	Description
<b>Upload quarantined files from the clients</b> (as of 14.3 RU2)	<p>When the client detects a risk and quarantines the file, the client notifies the management server. When this option is enabled, the management server automatically requests and retrieves the quarantined file. To view the quarantined file, use either the Risk log <b>Download file that the client quarantined</b> command or the REST API command, <code>GetFile</code>.</p> <p>If this option is disabled, you can select and retrieve individual files from the Risk log. You should disable this option if the file is too large or the client computer is offline. Files that are too large reduce the bandwidth.</p> <p>You can view which quarantined files have been retrieved by the management server from the client on the <b>Monitors &gt; Command Status</b> tab and marked with the <b>Get Suspicious File</b> command. For quarantined files on 14.3 RU1 MP1 and earlier clients, this command fails on non-portable executable (PE) files such as PDF files and scripts, such as PowerShell, JavaScript, and VBScript. The <code>Requested file not found</code> appears in the Command Status Details report.</p>

## Edit Domain Properties: Logon Banner

Use this tab to create and display a customizable message that all administrators should read before they can log on to the Symantec Endpoint Protection Manager Console. You can display any message. The most common purpose is to display a legal notice to tell the administrators that they are about to log on to a proprietary computer.

The message appears in the console after administrators type their user name and password and after they click **Log On**. After administrators have read the message, they can acknowledge the notice by clicking **OK**, which logs on the administrators. If administrators click **Cancel**, the logon process is canceled, and the administrator is taken back to the logon window. The message also appears if the administrator runs the reporting functions from a stand-alone Web browser that is connected to the management server.

**Table 344: Logon banner options**

Option	Description
<b>Provide a legal notice to administrators when they log on to the Symantec Endpoint Protection Manager</b>	Enables the message.
<b>Banner title</b>	Provides an optional title and intent of the message. For example, you can type a short title, such as NOTICE - PROPRIETARY SYSTEM. You may want to type the title in capital letters. The title can contain a maximum of 256 characters.
<b>Banner text</b>	Provides the content of the message. You can copy and paste a legal notice into the text field. The message can contain a maximum of 2048 characters.

---

## Domain Properties: Passwords

Table 345: Passwords

Option	Description
Allow users to save credentials when logging on	You can display the <b>Remember my user name</b> and <b>Remember my password</b> checkboxes on the Symantec Endpoint Protection Manager logon screen. If you enable this feature, the administrator's user name and password is prepopulated on the logon screen.
Allow never expiring passwords for administrators	If you check this box, you can set passwords to never expire for the administrators in the domain. After you check this box, the option to allow a never-expiring password appears in <b>Admin &gt; Administrators &gt; username &gt; Edit the Administrator &gt; Authentication</b> , where username is the administrator's user name. In that pane, you must then click <b>Password never expires</b> to enable a never-expiring password for that administrator. <a href="#">Enabling Symantec Endpoint Protection Manager logon passwords to never expire</a>

## Servers and Databases

### Servers

Use this pane to view and manage the sites, servers, and databases.

### Management Server

The Management Server pane provides general information about the management server.

Table 346: Management Server pane

Option	Description
Server Name	The name of the Symantec Endpoint Protection Manager server.
Version	The version number of the Symantec Endpoint Protection software.
Operating System	The operating system on which Symantec Endpoint Protection Manager is installed.
Address	The IP address of the server on which Symantec Endpoint Protection Manager is installed.
Start Time	The date and the time that the server was started.
Creation Time	The date and the time that the server was created.
Status	The current status of the server.

### Deny/Allow Console Access

The behavior of the Deny/Allow Console Access dialog box changes. These changes are based on the options that you previously checked in the **Server Properties** dialog box.

#### If you clicked:

- Granted Access in the **Server Properties** dialog box and then clicked Add or Edit, the Deny Console Access dialog box appears.
- Denied Access in the **Server Properties** dialog box and then clicked Add or Edit, the Allow Console Access dialog box appears.

---

## NOTE

Local addresses for the server on which Symantec Endpoint Protection Manager runs are always allowed, and are ignored if they are added to a list to deny access. Local addresses include 127.0.0.1, or the IP address for the server on which Symantec Endpoint Protection Manager runs.

**Table 347: Deny or Allow Console Access**

Option	Description
Single computer	If you clicked: <ul style="list-style-type: none"><li>Granted Access, then access to a specific management server from a remote management server console is automatically denied.</li><li>Denied Access, then access to a specific management server from a remote management server console is automatically allowed.</li></ul>
Group of computers	If you clicked: <ul style="list-style-type: none"><li>Granted Access, then access to a specific management server from a remote management server console is automatically denied.</li><li>Denied Access, then access to a specific management server from a remote management server console is automatically allowed.</li></ul>
IP address	Enables you to type the IP address of a single computer or the network IP address that is associated with a specific subnet. If you create exceptions for the computers that are assigned both an IPv4 and an IPv6 address, you must add separate exceptions for each.
Subnet mask	Enables you to type the subnet mask that is associated with the network address of a designated group of computers.

## Test Configuration

Type a user name and password to test an RSA Authentication Agent client.

## Edit IP Addresses

You can edit any IP address that appears in the dialog box. The IP addresses that appear in this dialog box are part of the exception list that is defined in the **General** tab of the **Server Properties** dialog box.

## Server Properties: General

This panel lets you set access to the management server for remote consoles and servers.

You can manage exceptions based on the IP address of a single computer or the subnet mask of a group of computers. If you create exceptions for the computers that are assigned both an IPv4 and an IPv6 address, you must add separate exceptions for each.

## NOTE

Local addresses for the server on which Symantec Endpoint Protection Manager runs are always allowed, and are ignored if they are added to a list to deny access. Local addresses include 127.0.0.1, or the IP address for the server on which Symantec Endpoint Protection Manager runs.

**Table 348: Server Properties**

Option	Description
<b>Description</b>	Lets you provide additional information about the management server.
<b>Server Communication Permission</b>	<p>Lets you specify which remote consoles and servers have access to the management server. You can configure the following options:</p> <ul style="list-style-type: none"> <li>• <b>Granted Access</b> Allows all computers to communicate with the management server.</li> <li>• <b>Denied Access</b> Blocks all computers from communicating with the management server</li> <li>• <b>Except those in the list below</b> Specifies the exceptions to the computers that have been granted or denied access globally. You define an exception by the IP address of a single computer or the subnet mask of a group of computers. If you create exceptions for the computers that are assigned both an IPv4 and an IPv6 address, you must add separate exceptions for each. The list of exceptions automatically denies access if you granted access to all consoles and servers. The list of exceptions automatically grants access if you denied access to all consoles and servers.</li> </ul>

## Server Properties: Email Server

The options on this tab configure a mail server so that notifications can be emailed to administrators when security events occur.

**Table 349: Email server options**

Option	Description
<b>Server address</b>	IP address, host name, or domain name of the mail server.
<b>Port</b>	Port number that is used for email on the mail server that sends the notifications.
<b>Sender email address</b>	<p>The email address from which notifications are sent.</p> <p>If you leave this box blank, the address is SEPM_Server@domain, where domain is the domain to which the email address of the default administrator belongs.</p>
<b>User name</b>	The user name that is used to authenticate to the mail server, if the server requires authentication.
<b>Password</b>	The password that is used with <b>Username</b> to authenticate to the mail server, if the server requires authentication.
<b>Require the specified email server to use a secure connection</b>	Check this box if your mail server requires a secure connection. TLS and SSL are two methods for encrypting the connection to the mail server over HTTPS. You must also configure your mail server to use TLS or SSL communication.
<b>Send Test Email</b>	Immediately tests the mail server and email address.

## Server Properties: Directory Servers

If your network includes directory servers, you can synchronize the data records about clients between the directory servers and Symantec Endpoint Protection Manager. You can include replication directory servers in your configuration. You can also set up a custom synchronization schedule.

### NOTE

Synchronization is only possible for Active Directory Servers. Symantec Endpoint Protection does not support synchronization with LDAP servers.

---

**Table 350: Directory Servers settings**

Option	Description
Name	Displays the names of directory servers and replication directory servers for which you set up synchronization. <b>Note:</b> If your directory server name includes certain special characters, you must escape the characters. <b>Note:</b> <a href="#">Importing organizational units from a directory server</a>
Type	Displays the type of protocol that has been set up between a directory server and a management server.
Properties	Displays the properties of the directory server.
Synchronize with Directory Servers	Enables you to synchronize data records between directory servers and a management server. This option is enabled by default whenever you add a directory server.
Auto-schedule (occurs every 24 hours)	Synchronizes records automatically every 24 hours between a directory server and a management server. The default setting for synchronization is set for every twenty-four (24) hours.
Synchronize every: hours	Sets up a customized schedule for the frequency with which you want to synchronize data records between a directory server and a management server. You can also edit the interval by editing the tomcat\etc\conf.properties file.

## Server Properties: Proxy Server

If your network includes HTTP or HTTPS proxy servers, you must establish a connection between the proxy server and Symantec Endpoint Protection Manager. The HTTP/HTTPS proxy server automatically connects to the Symantec subscription services.

You can also use an FTP proxy server to connect to Symantec subscription services.

**Table 351: Proxy server and Symantec Endpoint Protection Manager communication settings**

Option	Description
HTTP and HTTPS or FTP Proxy Settings	<p><b>Proxy usage</b> Specify whether or not you use the proxy server by selecting one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Use my Internet Options HTTP settings (LiveUpdate Only)</b> Use this default option so that the LiveUpdate server uses the Windows system proxy to connect to the Internet. You do not need to configure the proxy server settings. If you use this option, then the Symantec Endpoint Protection Manager cannot use a proxy server. Instead, the Symantec Endpoint Protection Manager must obtain the following information directly and not through a proxy server: <ul style="list-style-type: none"> <li>• Latest definition version available on LiveUpdate.</li> <li>• Latest threat risk categorization from Symantec.</li> </ul> <p><b>Note:</b> An internal LiveUpdate server cannot use HTTPs with a proxy in place. If there is a proxy, then you must configure HTTP for the internal LiveUpdate server.</p> </li> <li>• <b>Do not use a proxy</b> This setting is the default setting. All other settings are not applicable and they are disabled.</li> <li>• <b>Use custom proxy settings</b> If you use custom proxy settings, you can require authentication</li> </ul> <p><b>When Use custom proxy settings is selected, you must enter the following information:</b></p> <ul style="list-style-type: none"> <li>• <b>Server address</b> A valid IP address or host name of up to 256 characters for the HTTP/HTTPS proxy server.</li> <li>• <b>Port</b> The port number (0 – 65535) of the HTTP/HTTPS or FTP proxy server.</li> <li>• <b>Authentication needed to connect through the proxy server</b> Enables you to require authentication when the management server tries to connect.</li> <li>• <b>User name</b> The user name that is needed to connect to the HTTP/HTTPS proxy server or FTP server.</li> <li>• <b>Password</b> The password that is needed to connect to the HTTP/HTTPS proxy server.</li> <li>• <b>NT LAN Manager Authentication</b> Enables or disables NT LAN Manager (NTLM) Authentication. If you use NT LAN Manager Authentication, type <code>user@domain</code> or <code>domain\user</code> for the user name format.</li> </ul> <p>If you do not use this option, then LiveUpdate may fail.</p>

## Server Properties: File Fingerprint Update

You can automatically update the existing file fingerprint lists and the application lists that you use for system lockdown allow lists (whitelists) or deny lists (blacklists). The automatic update updates existing file fingerprint or application lists. It cannot upload a new list to the Symantec Endpoint Protection Manager console. Use the **File Fingerprint Update** tab to specify settings for the automatic updates.

### NOTE

These settings do not update any file fingerprint lists that you generate with the Collect File Fingerprint List command. File fingerprint lists that you generate with the command are automatically updated when you re-run the command on the same computer.



**Table 352: File fingerprint update settings**

Option	Description
<b>Automatically update the allow or deny lists</b>	Automatically updates existing file fingerprint lists and application lists for groups with system lockdown enabled. This command changed from <b>Automatically update the whitelist or blacklist</b> in 14.3 RU1.
<b>URL for index</b>	Specifies the location of the index.ini file. <a href="#">Creating an index.ini file for automatic updates of allow lists and deny lists that are used for system lockdown</a>
<b>Password for index</b>	If you use UNC or FTP, you must specify a password for the index file.
<b>URL for content</b>	The location of the zip file that contains the allow list or deny list content.
<b>User name for content</b>	If you use UNC or FTP, you must specify a user name for the zip file.
<b>Password for content</b>	If you use UNC or FTP, you must specify a password for the zip file.
<b>Auto-schedule</b>	Specifies that the update uses the default schedule.
<b>Update every</b>	Specifies a custom schedule for the updates.

## Add Directory Server: General

Before you can import users from any directory server, you need to establish communication protocols between the directory server and Symantec Endpoint Protection Manager.

With Active Directory servers, you cannot filter information about the users. With LDAP servers, you can filter the information about users before you import the data. Therefore you may want to add an Active Directory server that is LDAP-compliant as an LDAP server if you need to filter the data.

You must specify the names of the directory and other pertinent information before the connection between a directory server and the management server becomes operational.

You can also specify whether or not the communication between a directory server or a replication server and the management server is encrypted.

**Table 353: General tab**

Option	Description
<b>Name</b>	Enables you to type a name of the directory server that you want to add.
<b>Server Type</b>	Enables you to select the type of directory server that you plan to add. You can check Active Directory or LDAP.
<b>Server IP Address or Name</b>	Enables you to type the IP address, host name, or domain name of the directory server that you plan to add.
<b>LDAP Port</b>	Enables you to type the port number of the directory server that you plan to add. The default port number is 389.
<b>LDAP BaseDN</b>	Enables you to type the LDAP BaseDN of the LDAP server that you plan to add. These values cannot be changed if you add an Active Directory server.
<b>User Name</b>	Enables you to type the user name of the authorized directory server account.
<b>Password</b>	Enables you to type the password for the directory server account.
<b>Use Secure Connection</b>	Enables you to have the management server communicate with a directory server by using the Secure Sockets Layer (SSL). If this option is not checked, an unencrypted connection is used.

---

## Add Directory Server: Replication Servers

Use this tab to add directory servers to use for replication. You should add a management server to use if the connection to the first Active Directory server or LDAP server fails. The management server then goes to the addresses you added on the **Replication Servers** tab. When you add a replication server, you type the IP address or host name of the replication server.

## Database Server

The management server uses either the default Microsoft SQL Server Express database or Microsoft SQL Server.

**Table 354: Database Server pane**

Item	Description
Name	Lists the name of the computer on which the database is installed. The name for the SQL Server Express database is same as the computer name, or <code>SQLEXPRESSSYM</code> by default, and is automatically assigned if you selected default database during the installation. <b>Note:</b> In 14.3 MP1 and earlier the default embedded database was called <code>localhost</code>
Description	Displays a description of the database.
Database Address	Lists the IP address or the host name of the database.
Type	Lists the type of adapter used on the computer on which the database was installed.
Version	Lists the version of the database that was installed.
Database	Lists the name of the database. The default name is <code>sem5</code> .
Database User	Lists the name of the database user. The default user name for the database is <code>DBA</code> .
Creation Time	Lists the date and time that the database was created.

## Database Properties: General

Use this dialog box to set general database properties and to reduce the space the database takes.

**Table 355: Database options**

Option	Description
<b>Name</b>	Lets you enter a descriptive name or other useful identifier for the database.
<b>Description</b>	Lets you provide a more detailed description or enter other notes for the database.
<b>Truncate the database transaction logs</b>	Lets you schedule regular truncation of the database transaction logs. Use this setting to keep the logs a manageable size. The default schedule is every four hours.
<b>Rebuild indexes</b>	Lets you schedule a time when the database indexes get rebuilt. Reindexing improves database performance. The default schedule is every week at 2:00 A.M. on Sunday.

## Database Properties: Log Settings

The options on this tab control the amount of log data that is stored in the database for this site. You can set the number of entries that are kept in the database and the length of time that the entries are kept.

**Table 356: Risk Log options**

Option	Description
<b>Delete risk events after N days</b>	Specifies the number of days after which risk events are deleted from the database. The default value is 60 days.
<b>Delete acknowledged notifications after N days</b>	Specifies the number of days after which acknowledged notifications are deleted from the database. The default value is 30 days.
<b>Delete scan events after N days</b>	Specifies the number of days after which risk scans are deleted from the database. The default value is 30 days.
<b>Delete unused virus definitions</b>	<b>Specifies whether to delete the virus definitions that meet the following criteria:</b> <ul style="list-style-type: none"> <li>No computer currently uses them.</li> <li>They are not in the stored histories of computers from the database.</li> </ul> Unused definitions are deleted by default.
<b>Compress risk events after N days</b>	Number of days after which identical risk-found events are compressed into one event. The identical risk events that are found to occur within one-hour time intervals are compressed and counted. The infected file names are not compressed. The default value is 7 days.
<b>Delete unacknowledged notifications after N days</b>	Specifies the number of days after which unacknowledged notifications are deleted from the database. The default value is 30 days.
<b>Delete commands after N days</b>	Specifies the number of days after which the commands that you have run from the console are deleted from the database. This setting also deletes the status information about the commands. The default value is 30 days.
<b>Delete EICAR events</b>	Specifies whether or not to delete the virus events that contain EICAR as the name of the virus from the database. EICAR events are deleted by default. The EICAR virus is benign and is used for testing purposes. The EICAR test virus is a text file that the European Institute for Computer Antivirus Research (EICAR) developed. It provides a safe way to test most antivirus software. You can download it from the EICAR website. You can use it to verify that the antivirus protection portion of Symantec Endpoint Protection works.

## Database Properties: Backup Settings

You can schedule options for automatic database backups.

**Table 357: Database backup options**

Option	Description
<b>Backup server</b>	Lets you select on which management server you want to save the backup.
<b>Backup path</b>	The backup path is set during the server configuration after the initial installation. The backup path is the path that is specified as the Server Data Root in the Management Server Configuration Wizard. The pathname is then appended with \backup. By default, the path is C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\backup. The Server Data Root specifies where the database data is stored. You can change Server Data Root during the installation or the reconfiguration of a database. Changing the Server Data Root changes the location of database data as well as the backup data path.
<b>Back up logs</b>	Backs up the logs that are stored in the database.

Option	Description
<b>Number of backups to keep</b>	Specifies the number of backups that are automatically saved. If this number is exceeded, the oldest copy is removed. Use this option if your company policy requires it. Set this number to 1 to help keep the Microsoft SQL Server Express database size below the 10 GB maximum.
<b>Schedule Backups</b>	Lets you set up an automatic schedule to back up a database.

## Truncate Database Transaction Log

To decrease the connection time between the database and Symantec Endpoint Protection Manager, the management server periodically removes older entries from the transaction log at a scheduled time. You can perform this task manually at any time by clicking **Run**.

The transaction log file is located in: <installation directory>\tomcat\logs\TruncateTxnLogTask-0.log

You can also change the time for when the management server is scheduled to perform this task.

[Database Properties: Backup Settings](#)

[Scheduling automatic database maintenance tasks](#)

## Rebuild Indexes

To improve the connection time between the database and Symantec Endpoint Protection Manager, the management server rebuilds the database index at a scheduled time. You can perform this task manually at any time by clicking **Run**.

You can also change the time for when the management server is scheduled to perform this task.

[Database Properties: Backup Settings](#)

[Scheduling automatic database maintenance tasks](#)

## Add Certificate

You can add multiple certificates, one at a time, to the certificate list for a private Insight server.

**Table 358: Private Insight server certificate settings**

Option	Description
<b>Certificate name</b>	The name of the certificate that you want to add. The name appears in the <b>Certificate List</b> on the <b>Private Insight Server</b> tab.
<b>Certificate file</b>	The certificate file name. The certificate must be in X.509 format.

## Configure Symantec VIP Authentication

You can configure Symantec VIP to use two-factor authentication (2FA) when logging on to Symantec Endpoint Protection Manager.

### NOTE

Two-factor authentication is not supported over IPv6, or in a FIPS-enabled environment.

**Table 359: Symantec VIP authentication settings**

Option	Description
<b>PKCS Keystore File (.p12)</b>	The PKCS keystore file contains the certificates and private key that the Symantec VIP server requires for communication.
<b>Keystore Password</b>	The password for the selected keystore file.

## Configure Smart Card Authentication

For administrators who work for US Federal Agencies, you can set up smart card authentication so that they can log on to Symantec Endpoint Protection Manager using a smart card.

As a first step, use this dialog box to validate that a certificate file was issued by the correct authority. Later, at the point that the administrator logs on, the management server reads the smart card's certificate and validates it against these CA certificates. To validate a certificate file, the management server checks that the certificate file is not listed in a certificate revocation list (CRL) on the Internet.

[Configuring Symantec Endpoint Protection Manager to authenticate administrators who log on with smart cards](#)

**Table 360: Smart card authentication settings**

Option	Description
<b>Specify the paths for the root and/or intermediate certificate files</b>	Locate each root or intermediate certificate file that the management server needs to check. Include as many certificate files as you need to check for revocation, one for each smart card. You can specify certificate files in the following formats: .cer, .crt, .der, and .pem. To select multiple files, press <b>Ctrl</b> . To add the certificate files manually, type a comma between each certificate file. Make sure that all the certificate files are present on the management server computer that the administrator need to log on to. Otherwise, the administrator cannot log on.
<b>Specify the paths for the certificate revocation lists</b>	For the management servers that cannot access Internet, copy the CRL to this computer where they can access it and perform the validation check. In addition, you must configure the <code>conf.properties</code> file so that the management server looks for the CRL on the computer instead of on the Internet. <b>Note:</b> For the management servers that do have Internet access, you do not need to use this setting.

## Site properties and replication

### Local Site

Symantec Endpoint Protection Manager organizes installations of components into sites. A site includes:

- One or more management servers
- One database

They are typically located together at the same business location. Large enterprise corporations typically install many sites. The number of sites is usually related to the company having multiple physical locations, separate divisions, and areas on different subnets. The corporate management and the IT departments that are responsible for security management typically determine both the configuration as well as the number of sites.

A local site is located on the management server to which you are connected and logged on. Because you can log on remotely to a management server that is located in another city, the site may not be physically local. Remote sites are the

sites that are linked to the local site as replication partners. A system administrator can centrally manage the security of both the local and the remote sites from the management server console.

**Table 361: Local Site pane**

Option	Description
Site Name	Gives a name to the locate site.
Site Description	Provides a description of the local site.
Replication Site Count	Lists the number of available replication partners that are located at remote sites.
Creation Time	Lists the time and date when the site was created.

## Site Properties: General

Use this dialog box to set the general properties for a site.

**Table 362: Site configuration options**

Option	Description
<b>Site Name</b>	Displays the name of the site to which these settings apply. A site name must contain a maximum of 60 characters, and it cannot be blank. All characters are allowed.
<b>Description</b>	Lets you type a description for this site
<b>Console Timeout</b>	<p>Determines the time period after the console times out. When you enable this option, the administrator is automatically logged off the console after the console reaches the timeout limit. The default is one hour.</p> <p><b>Note:</b> If you connect to the management server by using the remote web console, the default timeout is 10 minutes.</p> <p><b>Note:</b> For more information, see: <a href="#">Configuring communication between the Symantec Endpoint Protection Manager and the remote web console</a></p>
<b>Keep track of every application that the clients run</b>	<p>This option lets you control application learning at the site level.</p> <p>To disable application learning for all clients in the site, clear the checkbox.</p> <p>To enable application learning, select the checkbox. You must then also enable application learning at the group level. This setting is available on the <b>Communications Settings</b> panel.</p> <p><a href="#">Communications Settings for &lt;group_name&gt;</a></p>
<b>Delete learned applications after x days</b>	<p>Use this option if you need to reduce the size of the default database size before you upgrade the management server. In 14.3 RU1 and later, the Microsoft SQL Server Express database must be 10 GB or less.</p> <p>Clients with application learning enabled track every application running on the computer and forward this information to the management server. The management server processes this application information and saves it in two database tables. The size of these tables range from a few GBs in small environments and tens of thousands of GBs in large environments.</p>
<b>Move Up and Move Down</b>	<p>Specifies which management server sends notifications and runs scheduled reports.</p> <p>This option ensures that all the management servers in the site do not run the same scheduled scans and send notifications simultaneously. The management console uses the first server in the list to send reports and notifications. If the server is not available, the console uses the next server in the list.</p>

---

## Site Properties: Passwords

Table 363: Administrator password settings

Setting	Description
<b>Allow administrators to reset the passwords</b>	If you have a system administrator account, you can let any administrators for the site to reset the Symantec Endpoint Protection Manager logon password for other administrators. This setting applies to administrators with a system, domain, or limited account. Administrators can click the <b>Forgot your password?</b> link on the logon panel to request a temporary password.

## Site Properties: Data Collection

Symantec Endpoint Protection Manager collects information about client computers, which includes information about malware and product features, and sends it to Symantec. You can use this tab to manage these server submissions. Client submissions of additional data are controlled on the **Clients** tab.

You also use this tab to manage the automatic submission of client logs for troubleshooting.

### NOTE

The data that Symantec telemetry collects may include pseudonymous elements that are not directly identifiable. Symantec neither needs nor seeks to use telemetry data to identify any individual user.

Table 364: Server Data Collection options

Option	Description
<b>Send pseudonymous data to Symantec to receive enhanced threat protection intelligence</b>	<p>Sends a report with pseudonymous information about the client computer to Symantec. Symantec uses the report to better understand various malware trends and how customers use particular product features.</p> <p><b>Note:</b> If Symantec Endpoint Protection Manager is enrolled in the cloud, this setting gets automatically turned on. The cloud console needs the telemetry information to do a better job of threat analysis. You can disable this setting again, but Symantec recommends that you leave it checked.</p>
<b>Let clients send troubleshooting information to Symantec to resolve product issues faster</b>	<p>Automatically collects data and logs about a client if it crashes or behaves abnormally. The log data is not anonymous.</p>

## Site Properties: Private Insight Server

You can specify information about how your client computers in the site connect to a private Insight server.

### NOTE

The options in this dialog override any group setting for private servers that you configure in the console on **Clients > Policies > External Communication Settings > Private Cloud**.

**Table 365: Private Insight server settings**

Option	Description
<b>Enable private Insight server</b>	When you enable this option, clients use the private Insight server to look up file reputation information. You must specify the <b>Name</b> , <b>Server URL</b> , and <b>Port</b> for the server. You can specify only one server.
<b>Name</b>	Required when <b>Enable private Insight server</b> is enabled. Specifies a name for the server that appears in the management console.
<b>Description</b>	Specifies an optional description of the private Insight server.
<b>Server URL</b>	Required when <b>Enable private Insight server</b> is enabled. Specifies the server URL using HTTP or HTTPS. The URL format should include the URI. Check the documentation for Symantec™ Insight for Private Clouds for more information about the private Insight server URI.
<b>Port</b>	Required when <b>Enable private Insight server</b> is enabled. Specifies the port for the server in the range 1 to 65535. By default, the HTTP port is 80. By default, the HTTPS port is 443.

## External Logging for site name: Log Filter

You can use this tab to select the logs that you want to export data from to a text file or Syslog server. For some logs, you must also check the severity levels of the events that you want to have exported. You can use the **General** tab to enable exporting and to limit the number of entries exported.

## External Logging for site name: General

You can use this tab to configure settings to export the data from some logs to a text file or to a Syslog server. The text file is referred to as a dump file. By default, no logs are sent. You can use the Log Filter tab to select the logs you want to export.

**Table 366: General export options**

Option	Description
<b>Update Frequency</b>	Specifies how frequently you want the exported data to be sent to the file or server.
<b>Master Logging Server</b>	Specifies the server you want to send logs to.
<b>Enable Transmission of Logs to a Syslog Server</b>	<p>Sends the data in the selected logs to a Syslog server.</p> <p><b>Note:</b> You must configure the Syslog server to receive these logs.</p> <p><b>The following fields must be configured:</b></p> <ul style="list-style-type: none"> <li>• <b>Syslog Server</b> Specifies the IP address or domain name of the Syslog server you want to receive the log data.</li> <li>• <b>Destination Port</b> Specifies the destination port that the Syslog server uses to listen for Syslog messages. You can select UDP or TCP as the protocol to use, and you can change the default port, if desired.</li> <li>• <b>Log Facility</b> Specifies the number of the log facility that you want to be used in the Syslog configuration file. Valid values range from 0 to 23.</li> </ul>
<b>Export Logs to a Dump File</b>	<p>Exports the Management Server and Client logs that were selected on the <b>Log Filter</b> tab to a text file.</p> <p><b>Limit Dump File Records</b> For each log displayed, specify the number of entries you want to limit the exported data to.</p>



---

## Replication Partners

You can view the replication partner sites that are associated with the local site.

**Table 367: Replication partner site options**

Option	Description
Site Name	Provides the name of the site.
Contact Server	Provides the host name or IP address of a server that is established as a replication partner.
Status	Provides the status of the last replication.

## Replication Partner Properties

Use this dialog box to view more information about the replication partner. You can also view this information in the **Edit Replication Partner Properties** dialog box.

## Replication Partner Properties for a Site

[Replication partner information](#) describes the properties you can modify for a replication partner.

### NOTE

You can only configure replication partner properties for the local site.

**Table 368: Replication partner information**

Option	Description
Partner Name	The name of the other site that this site replicates data with.
Replication Management Server List	The host name or IP address of the other management server that this site replicates data with.
<ul style="list-style-type: none"><li>• <b>Replicate logs from the local site to this partner site</b></li><li>• <b>Replicate logs from this partner site to the local site</b></li></ul>	<p>Log replication uses what is called hub and spoke replication. You designate one central site as the hub, with one or more remote, or child sites as the spokes. Hub and spoke replication is good for environments with faster network connections between hubs and slower connections between branch offices. The logs replicate from the hub server to the spoke servers and vice versa, but the logs do not replicate directly between two spoke servers. All log data from multiple sites is consolidated to the hub, which allows the administrator to log on to a Symantec Endpoint Protection Manager for that central site and see data for all the sites.</p> <p>For this topology, you must choose which management server acts as the hub.</p> <ul style="list-style-type: none"><li>• <b>Replicate logs from the local site to this partner site</b> The local site is a spoke and your site, the partner site, is the hub. You want the logs from the other sites to be replicated to your site, the hub.</li><li>• <b>Replicate logs from this partner site to the local site</b> The local site is the hub and your site, the partner site, is a spoke. You want logs from your site to be replicated to the hub.</li></ul> <p><b>Note:</b> When you enable these settings for the first time, the management server does not replicate log records for the time period before you enabled the settings.</p>

Option	Description
<b>Replicate client packages and LiveUpdate content between local site and this partner site</b>	Use this option only in very specific scenarios. For example, if you have two sites replicating, but only one of the sites can download LiveUpdate content, this option provides content to the replication site. For client packages and LiveUpdate content, neither replication site overrides the other. Instead they compare what each site has, and if one site has a package or piece of content the other does not, then it is shared. If all content and client packages match up, then nothing is exchanged.
<b>Schedule</b>	<ul style="list-style-type: none"> <li>• <b>Auto-replicate</b> Replicates the data between the two replication partners at an automatic interval, usually every 2 hours. The management server chooses when to replicate based on the amount of data in the databases and other factors.</li> <li>• <b>Replicate on a schedule</b> Specifies when you want replication to start at a time that is convenient for users. For example, you may want to replicate the data after business hours when the least number of users are on their computers. Replication automatically restarts in case the replication partner is turned off or replication failed. <ul style="list-style-type: none"> <li>— For daily replication and weekly replication, the end time marks the last time that replication is allowed to restart before the next scheduled replication time.</li> <li>— For hourly replication, replication continues to restart at the beginning of every hour until the end time. If replication overlaps into the subsequent hour, replication starts at the beginning of the next available hour. For example, if replication starts at 9:00 A.M. and finishes at 10:10 A.M., the next time replication starts is at 11 A.M.</li> </ul> </li> </ul>

## Remote Sites Management

You can manage remote sites in the Remote Sites Management pane. You perform the same tasks that you can perform for a local site, such as managing management servers. However, you can only add remote sites with the Management Server Configuration Wizard, a separate utility that is automatically installed during the initial installation.

### Tasks that you can perform regarding remote sites include:

- Delete a remote site and its replication partnerships.
- Change access to the console of the remote site.
- Set up the mail server for the remote site.
- Schedule directory server synchronization for the remote site.
- Set up a connection from the remote site's server to a proxy server.
- Configure external logging to send logs to a file or a Syslog server.

[Setting up sites and replication](#)

## Management Server Configuration Wizard

### Management Server Configuration

You use the Management Server Configuration Wizard to set up your management server and the associated database.

[About SQL Server database authentication modes](#)

[About SQL Server configuration settings](#)

## Creating the system administrator account and configuring the email server

### Creating the system administrator account

You create the system administrator account when you configure the management server for the first time.

**Table 369: System administrator account options**

Option	Description
<b>Company name</b> (optional)	Specifies your company name. This company name displays within Symantec Endpoint Protection Manager, both as a default domain property and in the details of the default administrator. If you use multiple domains within Symantec Endpoint Protection Manager, you can use a different company name for each domain for organizational purposes.
<b>User name</b>	Sets the default system administrator account name to <code>admin</code> . You cannot modify the default user name during installation.
<b>Password and Confirm password</b>	<p>Specifies your password for logging on to the management server.</p> <p><b>Password Strength</b> should be <b>Strong</b> or greater. You can create a strong password with the following guidelines:</p> <ul style="list-style-type: none"> <li>Strong passwords contain a minimum of eight characters.</li> <li>Strong passwords contain a combination of letters, numbers and at least one special character. If you install Symantec Endpoint Protection Manager with the default database: <ul style="list-style-type: none"> <li>For the Microsoft SQL Server database, passwords must be 8 through 30 characters in length, and cannot contain the following special characters: " ; and space.</li> <li>For the embedded database, passwords must be 6 through 30 characters in length, and cannot contain the following special characters: \ " ; and space.</li> <li>For the SQL Server database, the passwords must be six to 256 characters in length and can contain any character.</li> </ul> </li> <li>Strong passwords contain a combination of upper and lower case letters.</li> <li>Strong passwords do not contain repetitions or sequences of characters, such as <code>12345678</code> or <code>zzzzzzzz</code>.</li> <li>Strong passwords do not contain familiar words or phrases.</li> <li>Strong passwords do not contain the user name.</li> </ul> <p>By default, the password expires after 60 days, and is initially locked out for 15 minutes after five unsuccessful attempts. For security purposes, the lockout period is progressive, which means it doubles if you are locked out on a subsequent login attempt. The original lockout period restores after 24 hours, or if you successfully log on.</p> <p>If you forget the password later, you can request a temporary password by email.</p> <p><a href="#">Displaying the Remember my user name and Remember my password check boxes on the logon screen</a></p> <p><a href="#">Unlocking an administrator's account after too many logon attempts</a></p> <p><a href="#">Resetting a forgotten Symantec Endpoint Protection Manager password</a></p>
<b>Email address</b>	Enables you to receive system notifications about the status of client deployment and client protection. Also enables you to receive a temporary password if you forget or lose your password.

## Configuring the mail server

The management server uses a mail server to send default reports, notifications, or a temporary logon password. You can accept the default values to use the management server to send the email messages. To use a different mail server, check **Use a specified email server** and configure the settings in the fields provided.

Before you can proceed with management server configuration, you must test the server settings with **Send Test Email**, and then acknowledge when you receive of the test email. If you do not receive the test email, you can troubleshoot the failure on the mail server, and then continue the configuration process. If you do not correct the failure, you do not receive notifications, reports, or the email that provides a temporary logon password.

You can change the mail server settings at any time after the management server configuration is complete. You can change the settings through **Admin > Servers > server name > Edit the server properties**, where server name is the name of your management server. Click the **Email Server** tab.

**Table 370: Mail server settings**

Option	Description
<b>Email server IP address or name</b>	The IP address or name of the management server displays by default. If you want to use a different mail server, you can enter the relevant IP address, host name, or domain name here.
<b>Port number</b>	The port number that is used for email on the mail server that sends the notifications. Some networks block traffic on TCP port 25. If you have designated a port other than TCP port 25 for your mail server traffic, enter it here.
<b>Sender email address</b>	Specify the email address from which notifications are sent. If you leave this box blank, the address is SEPM_Server@domain, where domain is the domain to which the email address of the default administrator belongs.
<b>User name</b>	The user name that is used to authenticate to the mail server, if the server requires authentication.
<b>Password</b>	The password that is used with <b>Username</b> to authenticate to the mail server, if the server requires authentication.
<b>Require the specified server to use a secure connection</b>	Check this box if your mail server requires a secure connection, and then indicate which protocol is in use. You must also configure your mail server to use TLS or SSL communication.

[What are the types of notifications and when are they sent?](#)

## Selecting a configuration type

You select a configuration type when you configure the management server.

**Table 371: Management server configuration options**

Configuration Type	Details
<b>Default configuration for new installation</b>	Choose the default configuration if you want to use the default database with the default settings. The default database supports up to 5,000 clients. The default database is Microsoft SQL Server Express (14.3 RU1 and later), or the embedded database (14.3 MPx and earlier).
<b>Custom configuration for new installation</b>	Choose the custom configuration for more complex installation situations, such as: <ul style="list-style-type: none"><li>• To use a Microsoft SQL Server database: A Microsoft SQL Server database is required if you intend to manage more than 5,000 clients.</li><li>• To further customize the settings for an installation that uses the default database: For example, you may want to choose a different web console port instead of accepting the default of 9090.</li><li>• To install an additional management server for failover or load balancing to an existing site: The existing site must use a Microsoft SQL Server database (14.3 MPx and earlier), but can use either database for 14.3 RU1 and later.</li><li>• To configure a site for replication: Before you set up an additional site, make sure that you need to replicate data. <a href="#">Deciding whether or not to set up multiple sites and replication</a></li></ul>

Configuration Type	Details
<b>Recovery configuration</b>	<p>Enables you to reinstall or reconfigure the management server so it communicates with previously deployed clients. The primary contents of the recovery file include the following items:</p> <ul style="list-style-type: none"> <li>• The server private key (the Tomcat keystore)</li> <li>• The server private key password (to unlock the Tomcat keystore)</li> <li>• The Domain ID</li> <li>• The Apache SSL keys</li> <li>• Configured TCP port numbers and encryption password</li> </ul> <p>If you do not use the recovery file when you reinstall, you must reconnect the clients using the Client Deployment Wizard.</p> <p>By default, the file is located in the following directory, where timestamp represents when the file was created:  Drive:\Program Files\Symantec\Symantec Endpoint Protection Manager\Server Private Key Backup\recovery_timestamp.zip</p> <p><b>Note:</b> The recovery file does not include the server settings. When you reinstall Symantec Endpoint Protection Manager, you lose any server settings that you had previously changed. You can use the exported server properties file to reimport the server settings for recovery purposes.</p> <p><b>Recovery configuration</b> is checked if the Management Server Configuration Wizard detects a recovery file.</p> <p><a href="#">Restoring client-server communications with Communication Update Package Deployment</a></p> <p><a href="#">Exporting and importing server settings</a></p> <p><a href="#">Disaster recovery best practices for Endpoint Protection</a></p>
<b>Management server to manage fewer than 500 clients</b>	<p>This option determines the defaults for the management server configuration for the following settings:</p> <ul style="list-style-type: none"> <li>• Content revisions  For fewer than 500 clients, the default is 21 revisions.  For 500 or more clients, the default is 90 revisions.</li> <li>• Java Virtual Machine (JVM) heap sizes  For fewer than 500 clients, the default is a minimum of 512 MB and a maximum of 1024 MB.  For 500 or more clients, the default is a minimum of 1024 MB and a maximum of 2048 MB.</li> </ul> <p><a href="#">Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager</a></p>

## Selecting the type of database to use

You select one of the following options for the type of database that Symantec Endpoint Protection Manager uses. The database stores information about clients and settings for Symantec Endpoint Protection Manager.

**Table 372: Database settings**

Option	Description
<b>Default database</b>	<p>The default database is automatically installed with Symantec Endpoint Protection Manager. The default database supports up to 5,000 clients. The default database does not require configuration and is the easiest to install.</p> <p>The default database was the embedded database until 14.3 RU1, when the Microsoft SQL Server Express database replaced it.</p>
<b>Microsoft SQL Server database</b>	<p>Configures Symantec Endpoint Protection Manager to run with the Microsoft SQL Server database. Use Microsoft SQL Server if you must manage more than 5,000 clients. You must install Microsoft SQL Server before you install Symantec Endpoint Protection Manager. Additionally, the SQL Server client tools must be installed on the same computer where you install Symantec Endpoint Protection Manager.</p> <p>For a list of currently supported versions of Microsoft SQL Server, see the system requirements for this version of Symantec Endpoint Protection: <a href="#">Release notes, new fixes, and system requirements for all versions of Endpoint Protection</a> <a href="#">About SQL Server configuration settings</a></p>
<b>Database maintenance tasks</b>	<p>Specifies the following database maintenance tasks for the default database. You should not select the maintenance tasks if you use a Microsoft SQL Server database. These database maintenance tasks may conflict with any similar tasks that are configured in the SQL Server Management Studio.</p> <ul style="list-style-type: none"><li>• <b>Truncate the database transaction logs</b> The management server periodically removes older entries from the transaction log at a scheduled time. The default setting is every four hours.</li><li>• <b>Rebuild Indexes</b> The management server defragments the database table indexes to improve the time it takes to sort and search the database. The default setting is weekly at 2:00 A.M. on Sunday.</li></ul> <p>You can change the date, time, and frequency of the schedule for when the management server performs these tasks from the <b>Admin &gt; Servers</b> page. Click the database name, and then click <b>Edit Database Properties</b> under <b>Tasks</b>. <a href="#">Scheduling automatic database maintenance tasks</a></p>

## About creating an encryption password

For the encryption password, you either allow the management server to create a random password, or you create one for yourself. You should document the encryption password for future reference. You need the encryption password in case you need to perform disaster recovery. You cannot change the encryption password after you create it, unless you reinstall the management server.

If you forget the encryption password, you can recover it using the recovery file. Recovery files are saved to the directory `Drive:\Program Files\Symantec\Symantec Endpoint Protection Manager\Server Private Key Backup\` by default. Extract the contents of the .zip file. The encryption password appears within the `settings.properties` file.

**Table 373: Encryption password options**

Option	Details
<b>Use random password</b>	The management server creates a random password for you. The final panel before the database installation displays the random password.
<b>User defined</b>	You create the encryption password, which should contain between 6 and 32 characters. All characters are allowed. To create a strong password, you should use upper and lower case letters, numbers, and special characters. You should avoid any common words, sequences, or the repetition of characters.

[Disaster recovery best practices for Endpoint Protection](#)

## Specifying the database password during server reconfiguration

During the reconfiguration of the management server, you may be prompted to enter a database password.

Most of the settings that are shown cannot be modified during reconfiguration.

**Table 374: Database settings**

Option	Value
<b>Database server</b>	If this value is SQLEXPRESS\$SYMC, then the database is hosted on the same computer as the management server. Otherwise, this value reflects the name or IP address of the remote server hosting a SQL Server. The embedded database is called localhost (14.3 MPx and earlier).
<b>Database server port</b>	The port over which communication occurs between the management console Symantec Endpoint Protection Manager and the database. The default value is 2638. If you customized the port, it appears here.
<b>Database name</b>	The default value is sem5. If you customized the database name, it appears here.
<b>User</b>	The database user account. If you installed Symantec Endpoint Protection Manager with the default database, the value is DBA. If you installed Symantec Endpoint Protection Manager with a Microsoft SQL Server database, the default is sem5. If you customized the database user name, it appears here.

## Installing a new site as a replication partner to an existing site

[Server and replication options](#) describes the information you must provide when you install a new site as a replication partner to an existing site.

**Table 375: Server and replication options**

Option	Description
<b>Replication server</b>	The IP address, computer name, or fully qualified domain name of the existing server with which you want to replicate. <b>Note:</b> If the two servers are not in the same Windows domain, you may need to add host file entries on each server. These entries allow each server to resolve the other's fully qualified domain name.
<b>Replication server port</b>	The port over which replication occurs. The default value of 8443 appears, but if the existing server uses a custom port, enter it here.
<b>System Administrator name</b>	The System Administrator name to log on to the server. You cannot use Domain Administrator or Limited Administrator credentials.

Option	Description
<b>Password</b>	The password to authenticate the System Administrator name that you previously entered.
<b>Replicate Logs</b>	You can select more than one of the following options to replicate logs between sites, or select none: <ul style="list-style-type: none"> <li>Replicate logs from the local site to this partner site.</li> <li>Replicate logs from this partner site to the local site.</li> </ul>
<b>Replicate Client Packages and LiveUpdate content</b>	Replicates the client packages and the LiveUpdate content between the local site and this partner site.

## Installation Packages

### Client Install Packages: Overview

This pane lists details about the packages that are available for installation on the client computers.

**Table 376: Client install package details**

Column	Details
<b>Package Name</b>	The name of the package. You can customize this name.
<b>Platform</b>	The operating system onto which you can install the package.
<b>Type</b>	The type of client software that the package includes.
<b>Version</b>	The product version of the software that the package includes.
<b>Created Time</b>	The time and date on which the package was originally created.

### Client Install Settings: Overview

This pane lists the client installation type, based on how virus and spyware definitions are installed and updated on the client. These configurations apply only to Windows install packages, and only to 12.1.6 or later clients.

You cannot modify the settings for the default configuration.

### Client Install Feature Set: Overview

This pane lists which combinations of client features get installed on client computers. Client installation features are the security features and protection technologies that you can install on client computers.

Right-click on an existing feature set and then click **Edit** to see a feature tree for the set. The items under **Tasks** duplicate those in the contextual menu of the feature set.

You cannot modify the settings for the default feature sets.

## Client Install Settings

You add a new **Client Install Settings** or edit an existing one in the management console through **Admin > Install Packages > Client Install Settings > Tasks**. You specify the settings that affect how the client software is installed on client computers and the restart behavior after installation is complete. You must name each set of selections. You then select the setting name when you export the client installation package, or deploy a new client installation package using the Client Deployment Wizard.

When you click **Client Install Package > Export a Client Install Package**, you can select the package installation settings from within the **Installation Settings and Features** group box.



## NOTE

These settings apply only to Windows clients. Mac client computers always perform a hard restart after installation completes. Linux client computers do not restart after installation completes, and do not require a restart.

**Table 377: Basic Settings**

Setting	Options and Descriptions
Select an installation type	<p>Specifies the level of interaction the user has when the installation package installs on the client computer:</p> <ul style="list-style-type: none"><li>• <b>Interactive</b> Users interact with all installation dialog boxes. <b>Note:</b> If you use this setting, be aware that users are free to select a custom client software installation, and then install different components. <b>Note:</b> You should not use an interactive installation for remote deployment. This installation type fails unless users interact with it. Security features (such as Windows Session 0 isolation) on some operating systems may not allow the interactive installation wizard to appear. You should only use the interactive installation type for local installations.</li><li>• <b>Show progress bar only</b> Users see a Windows progress dialog box, but do not interact with the installation screens. This unattended setting is the default setting. <b>Note:</b> If you use this option, Windows may display to users one or more pop-up windows, and may not display the progress bar. This behavior is related to changes in Windows. However, the installation should succeed even if the user does not notice the pop-up windows.</li><li>• <b>Silent</b> Users do not see or interact with the installation dialog boxes. <b>Note:</b> You should use silent installations for remote deployment to minimize user disruption. <b>Note:</b> Silent installation requires any applications that plug into Symantec Endpoint Protection to be restarted, such as Microsoft Outlook.</li></ul> <p>These recommendations apply to both 32- and 64-bit operating systems.</p>
Installation directory settings	<ul style="list-style-type: none"><li>• <b>Install to the default installation folder</b> The default folder for 32-bit operating systems is C:\Program Files\Symantec\Symantec Endpoint Protection. The default folder for 64-bit operating systems is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection.</li><li>• <b>Install to a custom installation folder</b> Lets you change the installation folder. Do not install the client into the user's installation path, such as: "C:\Users\subfolder." There are situations when C:\Users is not the user's folder.</li></ul>
Install Standard client installation settings (uses cloud definitions)	<p>If you want to change between the Windows client installation types: <b>Standard client, Embedded or VDI, Dark network</b>, at a later time after client installation, you <b>must</b> first uninstall the existing client software, reconfigure these settings, and then reinstall the new client package.</p> <p>Installs a standard client. The standard client settings install only the current virus and spyware definitions. These clients are designed to check definitions in the cloud.</p> <p>When you upgrade clients, you should choose the standard client settings if you currently run the standard client with access to the cloud.</p> <p><a href="#">How to choose a client installation type</a></p>
Install Embedded or VDI client settings (uses cloud definitions)	<p>Installs an embedded or VDI client. The embedded or VDI client settings install only the current virus and spyware definitions. These clients are designed to check definitions in the cloud.</p> <p>For legacy reduced-size clients, choose the embedded client option.</p>

Setting	Options and Descriptions
<b>Install Dark network client installation settings (uses local definitions)</b>	Installs a dark network client. The dark network client installs with the full virus and spyware definitions, and uses definitions locally. These clients do not check definitions in the cloud If you have a dark network, you should upgrade your legacy standard-size clients to the dark network client.
<b>Do not uninstall existing security software</b>	The default setting for Windows client installation settings. Existing security software is not removed before the installation of Symantec Endpoint Protection.
<b>Automatically uninstall existing third-party security software</b>	Uninstalls third-party security software on the client computer before the installation of Symantec Endpoint Protection. This feature works for a fresh installation only, not an upgrade. To see which third-party software the client package removes, see: <a href="#">Third-party security software removal in Endpoint Protection 14</a> Some programs may have special uninstallation routines, or may need to have a self-protection component disabled. See the documentation for the third-party software.  <b>Note:</b> Changes to the third-party security software removal for version 14.2 mean that you cannot enable it for installation packages for earlier versions. For example, you cannot enable third-party security software removal for version 14.0.1 client packages if you create them with and deploy them from Symantec Endpoint Protection Manager version 14.2.  <a href="#">About the Symantec Endpoint Protection client preinstall removal feature</a> <a href="#">Configuring client packages to uninstall existing security software</a>
<b>Remove existing Symantec Endpoint Protection client software that cannot be uninstalled</b>	Uninstalls the existing Symantec Endpoint Protection client installation on the client computer, before the installation of Symantec Endpoint Protection. You should use this feature only to remove installations of the Symantec Endpoint Protection client that you cannot uninstall through standard methods. These methods include Windows Control Panel. You should not enable this feature for all deployments. This feature is comparable to CleanWipe.
<b>Enable installation logging</b>	Enables the installation log and writes it to the specified directory.
<b>Let computers automatically forward selected pseudonymous security information to Symantec</b>	Lets your client computers submit pseudonymous information about detected risks to Symantec Security Response. You can configure the client to submit the data based on detection type. The data that Symantec telemetry collects may include pseudonymous elements that are not directly identifiable. Symantec neither needs nor seeks to use telemetry data to identify any individual user. <a href="#">Understanding server data collection and client submissions and their importance to the security of your network</a>
<b>Add the program to the Start Menu</b>	Adds Symantec Endpoint Protection to the Windows <b>Start</b> menu.
<b>Upgrade settings</b>	<ul style="list-style-type: none"> <li>• <b>Maintain all logs, policies, and client-server communication settings</b> Use this option to keep the clients connected to the same management server and group as before.</li> <li>• <b>Remove all previous logs and policies, and reset the client-server communications settings</b> Use this option if you need to move the clients to a different management server or a new group.</li> </ul>

## Client Install Settings for Mac

**Table 378: Restart Settings**

Setting	Description
<b>Restart method</b>	<ul style="list-style-type: none"> <li>• <b>Forced restart</b> Use this option when the need to restart the computer is more important than the effect on the user. The user cannot delay the restart of their computer. This option is valuable when you mitigate a threat or preminent attack.</li> <li>• <b>Delayed restart</b> You can delay the client restart by an interval you select. Often you delay a restart to accommodate the needs of the user. You can allow the user to postpone when the computer restarts. The user is given five minutes to save any unsaved data.</li> <li>• <b>No restart</b> Use this option if there is no immediate threat or need to restart the client computer at a particular time. This option is a good choice when you can safely wait to restart the computer as part of the normal user routine. In some cases, you may be required to restart the client computer to start a service. You receive a notification when this requirement is present.</li> <li>• <b>Custom restart</b> Use this option when you need a combination of settings that the other restart methods do not provide.</li> </ul>
<b>Restart client computer</b>	<ul style="list-style-type: none"> <li>• <b>Immediately</b> Use this option when you must restart the client computer without delay. Situations that may require an immediate restart include malware remediation, schedule urgency, and proactive protection against an imminent threat. Use with <b>Forced Restart</b> for the most rapid computer restarts.</li> <li>• <b>At this time or Up to this time</b> Use this option when an immediate restart may affect work, or when you can safely delay the restart. Be sure that you understand the implications of delaying a restart when an active threat is present.</li> <li>• <b>Randomize the start time to be + or - 2 hours</b> Use this option to avoid conflicts with other scheduled tasks and to control client restart behavior. Restart randomization lets the clients restart at different times within a range of one to eight hours. This option is useful in virtualized environments to alleviate hardware overload. This overload can occur when all virtual machines that are hosted on a server restart at the same time.</li> </ul>
<b>Prompt</b>	<ul style="list-style-type: none"> <li>• <b>No prompt</b> This option is typically used with the <b>At this time</b> option to suppress the restart prompt during times when the user is away from the computer.</li> <li>• <b>Prompt with a countdown of</b> Use this option to display a prompt informing the user that a restart is imminent. This option is especially useful when used with the settings <b>Immediately</b> and <b>At this time</b>.</li> <li>• <b>Prompt and allow user to delay restart until</b> Use this option when you must restart the client computer within a given period of time. This option gives the user a chance to save data and exit programs, and ensures that they restart the computer.</li> </ul>
<b>Restart Message</b>	The message that appears in the prompt informs the user that the computer is about to restart.
<b>Other options</b>	<p>These options control the behavior of the client computer as it relates to other programs that may be running at the time of the restart.</p> <ul style="list-style-type: none"> <li>• <b>Hard restart</b> This option forces the client computer to restart regardless of any other activity occurring on the client computer. In most cases, you do not use this option except in extreme circumstances.</li> <li>• <b>Restart immediately if the user is not logged in</b> If the user is not logged in when the installation requests a restart, this option forces an immediate restart and overrides other pending restart actions.</li> </ul>

Restarting the client computers from Symantec Endpoint Protection Manager

## Client Install Feature Set

You add a new **Client Install Feature Set** or edit an existing one in the management console through **Admin > Install Packages > Client Install Feature Set > Tasks**. You select the protection features that get installed on client computers and save them as a set. You then select a feature name when you create 32-bit client software or 64-bit client software for Windows computers.

**Table 379: Client installation features**

Feature	Options and Descriptions
<b>Name and Description</b>	Provides the name and description that appear when you display the Export Package dialog box. If you open the Export Package dialog box when you click <b>Client Install Package &gt; Export Client Install Package</b> , you can select this feature set from the <b>Installation Settings and Features</b> group box. If you create a new package through the Client Deployment Wizard, you can select this feature set from the <b>Select Group and Install Feature Sets</b> group box, next to <b>Install Settings</b> .
<b>Feature set version</b>	New features are made available in new versions of the software but may not be compatible with installed clients of earlier versions. You can elect to use an older list of features to create client installation packages for these clients.
<b>Virus, Spyware, and Basic Download Protection</b>	<p>Enables the core virus and spyware protection, and basic download protection features. You can also select the following additional options:</p> <ul style="list-style-type: none"><li>• <b>Advanced Download Protection</b> Provides more comprehensive protection for downloads. Selecting this option produces a package that requires more network resources to deploy than the basic package.</li><li>• <b>Email Protection Scanners</b> Enables Auto-Protect for the selected email clients. You do not enable these features on mail servers. Also, POP3/SMTP Scanner, also known as Internet Email Auto-Protect, is not installed on server operating systems even if it is selected.</li></ul> <p><b>Note:</b> For client installation packages for mail servers, under <b>Virus, Spyware, and Basic Download Protection</b>, do not check the email scanner protection options. For client installation packages for workstations, check the email scanner protection option that applies to the mail server in your environment. For example, if you use a Microsoft Exchange mail server, check <b>Microsoft Outlook Scanner</b> for the client computers.</p> <p><b>Note:</b> You should install intrusion prevention on all workstations and laptops. Since intrusion prevention may cause performance issues on high-throughput servers, use caution when you deploy intrusion prevention to those servers.</p> <p><b>Note:</b> Symantec tested and certified the Virus and Spyware Protection components to use in the Federal Desktop Core Configuration (FDCC)-compliant environments.</p>
<b>Proactive Threat Protection</b>	<p>Enables Proactive Threat Protection and lets you enable the following options:</p> <ul style="list-style-type: none"><li>• <b>SONAR Protection</b> Enables the SONAR proactive threat scan client software. This software protects the processes that run on client computers against the attacks that are based on heuristic values rather than one-to-one signatures. Proactive Threat Protection also requires that you select Virus and Spyware Protection for installation.</li><li>• <b>Application and Device Control</b> Enables the protection technology that lets you control a variety of software applications and hardware devices on the client computers.</li></ul>

Feature	Options and Descriptions
<b>Network and Host Exploit Mitigation</b>	<p>Network and Host Exploit Mitigation includes the firewall, intrusion prevention, and Memory Exploit Mitigation, which protects against attacks before they enter the computer.</p> <ul style="list-style-type: none"> <li>The <b>firewall</b> allows the incoming network traffic and outgoing network traffic using firewall rules. The firewall and intrusion prevention block malware before it spreads to the computer and controls traffic.</li> <li><b>Intrusion prevention</b> intercepts data at the network layer. It uses signatures to scan packets or streams of packets. It scans each packet individually by looking for the patterns that correspond to network attacks or browser attacks. <ul style="list-style-type: none"> <li>IPS protects against some ransomware threats that traditional virus definitions alone cannot stop. IPS is the best defense against drive-by downloads, which occurs when software is unintentionally downloaded from the Internet. Attackers often use exploit kits to deliver a web-based attack through a drive-by download.</li> <li>In some cases, IPS can block file encryption by interrupting command-and-control (C&amp;C) communication. A C&amp;C server is a computer controlled by an attacker or cybercriminal and that is used to send commands to systems compromised by malware and receive stolen data from a target network.</li> <li>URL reputation prevents web threats based on the reputation score of a web page.</li> </ul> </li> </ul> <p>Note: To use custom IPS signatures, you must install the firewall.</p> <ul style="list-style-type: none"> <li><b>Memory Exploit Mitigation</b> protects against known vulnerabilities in unpatched software, such as JBoss or the Apache web server, which attackers exploit.</li> </ul>
<b>Application Hardening</b>	<p>Enables the application hardening feature, which is part of the Symantec Endpoint Security Complete product. Application hardening isolates applications from threats on Windows clients. It also monitors and blocks suspicious behavior in commonly used applications such as browsers, Microsoft Office, and Adobe Acrobat.</p> <p><b>Note:</b> Symantec Endpoint Protection Manager must be enrolled in the ICDm cloud console for this feature to run. You must also acquire a subscription to Symantec Endpoint Security Complete.</p> <p>This feature runs on the majority of the operating systems that the Symantec Endpoint Protection client runs with a few exceptions. For information about the system requirements, see: <a href="#">System requirements for Symantec Endpoint Protection Hardening</a></p>
<b>Endpoint Threat Defense for AD</b>	<p>Enables Symantec Endpoint Threat Defense for Active Directory functionality into the Symantec Endpoint Protection client to protect against the threats that target Active Directory.</p>
<b>Web and Cloud Access Protection</b>	<p>Web and Cloud Access Protection redirects Internet traffic to Windows and Mac client computers to the Symantec Web Security Service (WSS). When a user accesses a website using a web browser, the browser sends all web browser traffic through the nearest cloud-hosted Web Security Service, where network-based security policies are enforced. The Symantec WSS proxy can redirect, allow, or block the traffic. This feature requires licensing for Symantec Web Security Services. If you select this protection without selecting any other protections, 14.3 MP1 and earlier clients receive Host Integrity protection only.</p>

## Add a Client Install Package

This dialog box lets you add packages to the Symantec Endpoint Protection Manager so that you can configure and export them for client installation or upgrade. You can add the packages that you receive from Symantec, which contain the latest software. Packages can be .info or .zip files. You cannot add patches.

**Table 380: Add new software package**

Settings	Options and Descriptions
<b>Specify a name for this package</b>	Name of the package as it appears in the console after you add it.
<b>Specify the source folder for the package files</b>	Lets you browse to the package to add.
<b>Description</b>	Description of the package that appears in the console.

## Export Package settings

This dialog box lets you create custom client installation package files. Different settings are available for Windows clients, Mac clients, and Linux clients.

You can export Windows packages as a single executable file, or as a collection of files suitable for distribution through a third-party deployment tool.

### NOTE

The Mac and Linux client install packages automatically export in the `.zip` archive file format. To correctly preserve the file permissions, you should expand the archive file with an archive program native to the operating system. For example, use the Mac Archive Utility or the `ditto` command. You cannot use the Mac `unzip` command, a third-party application, or any Windows application to expand the files for these operating systems.

If you upgrade from a previous version, the Mac client package pathname is too long, and the export fails. You must choose a shorter pathname for a Mac client package.

The following table describes the settings for exporting Windows, Mac, and Linux client installation files.

**Table 381: Export package settings**

Setting	Options and Descriptions
<b>Export folder</b>	Windows, Mac, and Linux. Browse to and select the folder to contain the exported installation file. If you specify a folder that does not exist, the export process creates it for you. <b>Export Package</b> does not support directories with double-byte or high-ASCII characters, and blocks their selection. The export process creates nested folders within this folder and places the installation files in thee nested folders. For example, if you create an installation package for a group named <b>My Group</b> beneath <b>My Company</b> , a folder named <b>My Company_My Group</b> is created. This folder contains the exported installation package.
<b>Create a single .EXE for this package</b>	Windows only. Creates a single executable file for installation. Single executables are not supported with an Active Directory group policy installation or auto-upgrade by using Symantec Endpoint Protection Manager.
<b>Version Selection</b>	Windows only. Specifies a particular build for the installation (as of 14.3 RU2). Symantec installs new features and client patches regularly, between RUX releases. You can have an older management server and a more recent client.

Setting	Options and Descriptions
<b>Installation Features and Settings</b>	<p>Windows only. Installation settings for Mac computers apply only to AutoUpgrade.</p> <ul style="list-style-type: none"> <li>• <b>Maintain existing client features when updating</b> (as of 14.3 RU1 MP1) Keeps the currently installed client features from the previous release. Features remain installed on the client even if they are different from the features in the upgrade package. This setting is enabled by default. Uncheck this box to select a different set of features from <b>Select the security features for this package</b>.</li> <li>• <b>Select the security features for this package</b> Client installation feature sets that you configured and named, along with built-in feature selections. Client installation features determine which client software components install.</li> <li>• <b>Select the installation settings for this package</b> Client installation settings that Symantec Endpoint Protection Manager includes by default, or that you configured and named. Installation settings affect the end-user experience during the installation. For example, the settings may require user interaction with the installation, or that the installation forces a restart when it completes. Installation settings also define whether the installation package installs the standard, embedded/VDI, or dark network client. <a href="#">How to choose a client installation type</a></li> <li>• <b>Include virus definitions in the client installation package</b> Check this option to include the virus definitions with the client installation package. Uncheck this option in situations where the network has low bandwidth. As soon as the client connects to the management server, the client receives the full set of virus definitions.</li> </ul>
<b>Export Settings or Group Membership</b>	<p>Applies to Windows, Mac, and Linux, except where noted.</p> <ul style="list-style-type: none"> <li>• <b>Export a managed client</b> Lets you export a managed package that contains the default security policies. After you deploy this package, you can automatically manage the clients with the Symantec Endpoint Protection Manager console.</li> <li>• <b>Export an unmanaged client</b> Lets you export an unmanaged package that contains the default security policies. After you deploy this package, you cannot manage the clients with the Symantec Endpoint Protection Manager console. For Mac and Windows, you can convert an unmanaged client to a managed client at any time with <b>Communication Update Package Deployment</b> through the <b>Client Deployment Wizard</b></li> <li>• <b>Export packages with policies from the following groups</b> (Windows and Linux only) For Windows, this setting lets you export a managed or unmanaged package with security policies from a specific group or groups. If you select multiple groups, the export process creates a separate subdirectory of installation files for each group. After you deploy the exported client software, the managed client computers automatically appear in the group that you selected for installation. For Linux, this setting is only available if you export an unmanaged package. Default security policies apply if you uncheck this setting.</li> <li>• <b>Add clients automatically to the selected group. Existing clients remain in their current group.</b> (Windows only) Automatically adds the new clients to the selected group after the installation of the managed package.</li> </ul>
<b>Policy Mode</b>	<p>Windows only. Symantec recommends that you always use computer mode.</p> <ul style="list-style-type: none"> <li>• <b>Computer mode</b> Specifies that policies in the client installation package apply to computers as they authenticate to Symantec Endpoint Protection Manager. This setting is recommended for first-time installations.</li> <li>• <b>User mode</b> Specifies that policies in the client installation package apply to users as they log on to computers and authenticate to Symantec Endpoint Protection Manager.</li> </ul>



Setting	Options and Descriptions
Upgrade settings	Windows and Mac only. This setting lets you maintain current logs, policies and client-server communication settings, or remove previous logs and policies, and reset the client-server communication settings.

## Client Install Package Properties

This dialog box describes the relevant client installation package properties. You can change the name and description.

## Management Server List for list name

This dialog box shows you the failover and load balancing servers with which this software package communicates if you select this management server list. Priority number 1 indicates load balancing servers. Priority numbers greater than 1 indicate failover servers.

## Add Client Install Package: General

This dialog box lets you select the package to distribute, the components in the package to distribute, the install settings, and when to distribute.

### NOTE

If you display this help topic from the **Upgrade Clients with Package** wizard, your settings from the **General** tab are for **Maintain existing client features when updating** and **Upgrade Schedule** only.

**Table 382: General upgrade configuration settings**

Option	Description
<b>Select the package to use for upgrading clients in this group</b>	Lets you select the package for AutoUpgrade. By default, if a client runs a feature that is not in an upgrade package, the feature is uninstalled unless you check <b>Maintain existing client features when updating</b> .
<b>Version Selection</b>	<ul style="list-style-type: none"> <li>Displays a list of available Windows client installation packages that LiveUpdate downloads to the management server between releases (as of 14.3 RU2). LiveUpdate downloads installation packages with product improvements or critical security fixes. These packages do not include major features, such as what a release update (RUs) or maintenance patch (MPs) includes.</li> <li><b>Upgrade to English if unsupported language is unavailable</b> (Windows only) In 14.3 RU2 or later, Symantec Endpoint Protection is translated into the following languages only: English, French, Japanese, Brazilian Portuguese, and Spanish. If you check this option, all clients with an unsupported language are automatically upgraded to English, regardless of their language. <ul style="list-style-type: none"> <li>This option is available in an English Symantec Endpoint Protection Manager only. The clients continue to upgrade in the same language they used before. If you keep this option unchecked, clients with unsupported languages would not upgrade, because the unsupported client package does not exist. For example, an Italian 14.3 RU1 client would not get upgraded and would stay as version 14.3 RU1.</li> <li>If your client language is unsupported, check this option to automatically upgrade clients to English. For example, an Italian client would upgrade to English.</li> </ul> <p>You can include clients with multiple languages in a single group. For example, if a group has both French and Japanese clients, the French clients upgrade to English and the Japanese clients upgrade to Japanese.</p> <p>If you want to upgrade a client with a non-supported language to a supported language other than English (such as German to French), upgrade it manually.</p> </li> </ul>



Option	Description
Client Settings	<ul style="list-style-type: none"> <li>• <b>Maintain existing client features when updating</b> (Windows only) Keeps the currently installed client features from the previous release. Features remain installed on the client even if they are different from the features in the upgrade package. Uncheck this box to select a different set of features from <b>Select the features you want to use</b>: <ul style="list-style-type: none"> <li>– <b>Full Protection for Clients</b> Includes all protection technologies. Appropriate for laptops and desktops. Includes <b>Advanced Download Protection</b> and all client email scanners.</li> <li>– <b>Full Protection for Servers</b> Includes all protection technologies except all client email scanners. Appropriate for any servers that require maximum network security.</li> <li>– <b>Basic Protection for Servers</b> Includes only <b>Virus, Spyware, and Basic Download Protection</b>. Appropriate for any servers that require maximum network performance.</li> <li>– <b>Protection for Active Directory</b> Includes Symantec Endpoint Threat Defense for Active Directory functionality to protect against the threats that target Active Directory.</li> </ul> <a href="#">Client Install Feature Set</a> Any additional feature sets that you previously created under <b>Admin &gt; Install Packages &gt; Client Install Feature Sets</b> appear in the list for you to select. Some security features are not supported on all platforms. See: <a href="#">A new feature is installed even though the Auto-upgrade was set to maintain existing features Symantec Endpoint Protection features based on platform</a>  <b>Note:</b> Symantec Endpoint Protection Hardening is installed automatically even if it was not installed previously and this option is checked (as of 14.2). </li> <li>• <b>Install Settings</b> <ul style="list-style-type: none"> <li>– For Windows, this option defines the installation settings and upgrade settings, and the restart settings for when the installation is complete. For Windows, <b>Default Standard client Installation Settings</b> is selected by default.</li> <li>– For Mac, this option defines the upgrade settings and the restart settings for when the installation is complete.</li> </ul> Any additional install settings that you previously created under <b>Admin &gt; Install Packages &gt; Client Install Settings</b> appear in the list for you to select. You can only select Windows client settings for Windows packages, and Mac client settings for Mac install packages. </li> <li>• <b>Include new content types in the client installation package</b> Includes the new content that changed from a previous release. New content includes either new features or changes to existing features that require new content. For example, the content might be incompatible definitions from a previous release. If you use this option, the installation package is larger, but the client has the most current content immediately after the upgrade. If you do not use this option, the package is smaller, but the client must get content updates after installation with LiveUpdate or with Symantec Endpoint Protection Manager. A client's current version must be present in the Symantec Endpoint Protection Manager's install package to take advantage of this feature. For example, to include definitions in an installation package to upgrade from 12.1.x to 14, you must also have the 12.1.x client installation package stored in Symantec Endpoint Protection Manager. This additional requirement is necessary because of the change in definitions from version 12.1.x to version 14.x.  For information on which features are supported on the Windows, Mac, and Linux clients, see: <a href="#">Symantec Endpoint Protection features based on platform</a> <a href="#">Importing client installation packages into Symantec Endpoint Protection Manager</a> <a href="#">How to choose a client installation type</a> </li> </ul>

Option	Description
<b>Download Source</b>	<ul style="list-style-type: none"> <li>• <b>Download the client package from the management server</b> Downloads the package from Symantec Endpoint Protection Manager.</li> <li>• <b>Download the client package from the following URL (http or https):</b> Downloads the package from a web server that you have previously configured with the update. This update must be a single executable file or a compressed file. These files must be exported from Symantec Endpoint Protection Manager. Only HTTP and HTTPS are supported.</li> </ul>
<b>Upgrade Schedule</b>	<p>Lets you control the time of the client computer upgrade.</p> <ul style="list-style-type: none"> <li>• <b>From, To</b> Specifies a range of time over which to install packages. If the <b>From</b> and <b>To</b> times match, the upgrades start immediately.</li> <li>• <b>Distribute upgrades over</b> Specifies the number of days over which the packages can be distributed. The following formula calculates time:  <math display="block">(\text{Package Size} / \text{Server Transfer Rate}) * \text{Number of Computers}</math> </li> </ul> <p>As</p> $\text{MB} / \text{MB per second} * \text{Num} = \text{seconds}$

## Set User Information Collection

This dialog box lets you prompt users to type information about themselves during the client software installation process. This information appears in the **Properties** dialog box for each user and computer. After you collect this information, you must maintain and update it manually.

### NOTE

The first time you enable this option, the **Update User Information** dialog box appears on the client computer. However, if you edit one of the fields, the dialog box does not reappear. The only way the user knows that you want to have new information is if they inadvertently open the **Update User Information** dialog box.

**Table 383: User Information Collection**

Settings	Options and Descriptions
<b>Collect User Information</b>	Displays a dialog box that prompts users to type information about themselves.
<b>Pop-up Message</b>	This message appears at the top of the dialog box that explains to users what to type.
<b>Enable Remind Me Later</b>	Lets the users delay completing the dialog box for the specified amount of time in minutes.
<b>Select the fields for which the user provides input.</b>	The input fields (boxes) that the dialog displays to users.
<b>Optional</b>	Lets the users optionally type information in the associated field name.

## Add Client Install Package: Notification

This dialog box lets you specify whether to notify the users of a software upgrade, and whether they can postpone the upgrade.

---

**Table 384: Notification update configuration settings**

Setting	Description
<b>Notify users before an upgrade</b>	Lets you send a default message or a customized message that users see before the upgrade begins. The maximum message size is 128 characters and 2 lines.
<b>Use Default</b>	Resets the notification message to the default message.
<b>Allow users to postpone the upgrade process</b>	When notification is enabled, you can optionally allow users to postpone the upgrade for a configurable amount of time. The <b>Minimum Time</b> and <b>Maximum Time</b> menus provide a range of values.

## Client Install Settings for Mac

You add a new **Client Install Settings** or edit an existing one in the management console through **Admin > Install Packages > Client Install Settings > Tasks**. You specify the upgrade settings and the settings that affect the restart behavior after the upgrade is complete. These settings only apply to an upgrade, and do not apply during the creation of a new client installation package.

You must name each set of selections. You select the setting name when you use the **Upgrade Clients with Package** wizard to automatically upgrade the clients

[Upgrade Settings for Mac](#)

**Table 385: Restart Settings for Mac**

Setting	Description
<b>Restart method</b>	<ul style="list-style-type: none"> <li>• <b>Forced restart</b> Use this option when the need to restart the computer is more important than the effect on the user. The user cannot delay the restart of their computer. This option is valuable when you mitigate a threat or preeminent attack.</li> <li>• <b>Delayed restart</b> You can delay the client restart by an interval you select. Often you delay a restart to accommodate the needs of the user. You can allow the user to postpone when the computer restarts. The user is given five minutes to save any unsaved data.</li> <li>• <b>No restart</b> Use this option if there is no immediate threat or need to restart the client computer at a particular time. This option is a good choice when you can safely wait to restart the computer as part of the normal user routine. In some cases, you may be required to restart the client computer to start a service. You receive a notification when this requirement is present.</li> <li>• <b>Custom restart</b> Use this option when you need a combination of settings that the other restart methods do not provide.</li> </ul>
<b>Restart client computer</b>	<ul style="list-style-type: none"> <li>• <b>Immediately</b> Use this option when you must restart the client computer without delay. Situations that may require an immediate restart include malware remediation, schedule urgency, and proactive protection against an imminent threat. Use with <b>Forced Restart</b> for the most rapid computer restarts.</li> <li>• <b>At this time or Up to this time</b> Use this option when an immediate restart may affect work, or when you can safely delay the restart. Be sure that you understand the implications of delaying a restart when an active threat is present.</li> <li>• <b>Randomize the start time to be + or - 2 hours</b> Use this option to avoid conflicts with other scheduled tasks and to control client restart behavior. Restart randomization lets the clients restart at different times within a range of one to eight hours. This option is useful in virtualized environments to alleviate hardware overload. This overload can occur when all virtual machines that are hosted on a server restart at the same time.</li> </ul>
<b>Prompt</b>	<ul style="list-style-type: none"> <li>• <b>No prompt</b> This option is typically used with the <b>At this time</b> option to suppress the restart prompt during times when the user is away from the computer.</li> <li>• <b>Prompt with a countdown of</b> Use this option to display a prompt informing the user that a restart is imminent. This option is especially useful when used with the settings <b>Immediately</b> and <b>At this time</b>.</li> <li>• <b>Prompt and allow user to delay restart until or Prompt and allow snooze up to</b> Use this option when you must restart the client computer within a given period of time. This option gives the user a chance to save data and exit programs, and ensures that they restart the computer.</li> </ul>
<b>Restart Message</b>	The message that appears in the prompt informs the user that the computer is about to restart.
<b>Other options</b>	<p>These options control the behavior of the client computer as it relates to other programs that may be running at the time of the restart.</p> <ul style="list-style-type: none"> <li>• <b>Hard restart</b> This option forces the client computer to restart regardless of any other activity occurring on the client computer. In most cases, you do not use this option except in extreme circumstances.</li> <li>• <b>Restart immediately if the user is not logged in</b> If the user is not logged in when the installation requests a restart, this option forces an immediate restart and overrides other pending restart actions.</li> </ul>

---

**Table 386: Upgrade Settings for Mac**

Setting	Options and Descriptions
Upgrade settings	<ul style="list-style-type: none"><li>• <b>Maintain all logs, policies, and client-server communication settings</b> Keeps all logs and previous update settings. Keeps the communication settings with the management server.</li><li>• <b>Remove all previous logs and policies, and reset the client-server communications settings</b> Deletes and replaces all logs and previous settings. Deletes and replaces the management server communication settings.</li></ul>

[Upgrading client software with AutoUpgrade](#)

## Monitoring and Reports

### Home page

The customizable **Home** page contains important information about the security status of your network.

If your administrator account does not have permission to view reports, your **Home** page does not contain the automatically generated reports.

[Adding an administrator account and setting access rights](#)

Table 387: Home page items and reports

Report or Status Information	Description
<b>Security Status</b>	<ul style="list-style-type: none"> <li>• <b>Security Status - Good or Attention Needed.</b> The thresholds that you set on the <b>Preferences &gt; Security Status</b> tab determine the definitions of <b>Good</b> and <b>Attention Needed</b>.</li> <li>• <b>Preferences</b> Lets you change some of the default options that appear for the <b>Security Status</b> panel, the Home and Monitors tabs, and the logs and reports. <a href="#">Configuring reporting preferences</a></li> <li>• <b>No unacknowledged notifications in the last 24 hours</b> When a certain condition is met or a specified action is performed, the management server generates a notification. An unacknowledged notification is a notification that you do not read within 24 hours of receiving it. <a href="#">Viewing and acknowledging notifications</a> If you have a system administrator account, you can click the <b>Preferences</b> link and use the <b>Home</b> and <b>Monitors</b> tab to change this notifications display. You can set up notifications that the management server does not automatically generate. <a href="#">Setting up administrator notifications</a></li> </ul>
<b>Endpoint Status</b>	<p>Displays the overall system protection status for endpoints on your network.</p> <ul style="list-style-type: none"> <li>• <b>Up-to-date</b> The number of endpoints that have definitions that are current.</li> <li>• <b>Out-of-date</b> The number of endpoints that have definitions that are out of date.</li> <li>• <b>Offline</b> The number of endpoints that are offline.</li> <li>• <b>Disabled</b> The number of endpoints that are disabled. Endpoints report <b>Disabled</b> when a malfunction or when user action disables one or more protection technologies. If an administrator policy disables endpoints, those endpoints do not display in this chart.</li> <li>• <b>Host Integrity Failed</b> The number of endpoints that failed the Host Integrity check. This number is always zero if you do not have Host Integrity enabled.</li> <li>• <b>Computers needing a restart</b> Click the number to see which computers need a restart.</li> </ul>
<b>License Status</b>	<p>This report displays the licensing information for trial licenses and paid licenses. Click <b>Licensing Details</b> to view a report that contains detail information for all licenses.</p> <p><a href="#">How to manage the license count for non-persistent VDI clients</a></p> <p><a href="#">Purging obsolete non-persistent VDI clients to free up licenses</a></p>
<b>Symantec Security Response</b>	<p>The Security Response section shows the ThreatCon meter, which indicates the current severity level of threat to computers in a network. The severity levels are based on the threat assessments that Symantec Security Response makes. The ThreatCon severity level provides an overall view of global Internet security.</p>

Report or Status Information	Description
<b>Activity Summary: Virus and Risks</b>	<p>Displays an activity summary for the last hour and by the infection count for viruses and security risks. You can change the time interval for the detection count. For example, you can select <b>Last 24 hours</b>.</p> <p>Click <b>Preferences &gt; Home and Monitors</b> to change the time interval and detection count display.</p> <p>The Activity Summary by Detection Count summarizes the following information:</p> <ul style="list-style-type: none"> <li>• A count of the actions that have been taken on viruses and security risks.</li> <li>• The incidence of new virus and security risk detections.</li> <li>• The number of computers that remain infected by viruses and security risks.</li> </ul> <p>The Activity Summary by Number of Computers summarizes the following information:</p> <ul style="list-style-type: none"> <li>• The number of distinct computers on which the various actions have been performed on viruses and security risks.</li> <li>• The total number of new virus and security risk detections.</li> <li>• The total number of computers that still remain infected by viruses and security risks.</li> </ul> <p>For example, suppose you have five Cleaned actions in the Detection Count view. If all of the detections occur on the same computer, then the Number of Computers view shows a count of one, not five.</p> <p><b>Suspicious</b></p> <p>Shows that a SONAR scan has detected something that you should investigate. It may or may not be harmless. If you determine that this risk is harmless, you can use the Exceptions policy to exclude it from detection in the future. If the detection action for the risk is Log only, and you determine that this risk is harmful, you can use the Exceptions policy to terminate or quarantine the risk. If Symantec Endpoint Protection cannot remediate this risk, you might need to remove the risk manually.</p> <p><b>Newly Infected/Still Infected</b></p> <p>Shows the number of risks that have infected computers during the selected time interval only. Newly Infected is a subset of Still Infected. The Still Infected count shows the total number of risks that a scan would continue to classify as infected, also within the configured time interval. For example, the computer may still be infected because Symantec Endpoint Protection can only partially remove the risk.</p> <p>Both the Newly Infected count and the Still Infected count show the risks that require you to take some further action to clean. In most cases, you can take this action from the console and do not have to go to the computer.</p> <p><b>Note:</b> A computer is counted as part of the Newly Infected count if the detection event that occurred during the time range of the Home page. For example, if an unremediated risk affected a computer within the past 24 hours, the Newly Infected count goes up on the Home page. The risk can be unremediated because of a partial remediation or because the security policy for that risk is set to Log only.</p> <p>You can determine the total number of events that have occurred in the last time period configured to show on the Home page. To determine total number, add the counts from all rows in the Activity Summary except for Still Infected.</p>
<b>Activity Summary: Exploits</b>	Displays an activity summary for the last hour of detections made by Memory Exploit Mitigation. You can change the time interval for the detection count. For example, you can select <b>Last 24 hours</b> .
<b>Favorite Reports</b>	The Favorite Reports section contains some default reports, including a Memory Exploit Mitigation Detections report. You can customize this section by replacing one or more of these reports with any other default report or custom report that you want. Favorite reports run every time you view them so that their data is current.

## Preferences: Home page and Monitors page

You can use the **Home and Monitors** tab to change the default options for the following items.

**Table 388: Home page and Monitors page Summary tab display options**

Option	Description
<b>Time range</b>	Specifies the unit of time that is used in the reports that appear on the <b>Home</b> page and <b>Monitors</b> page <b>Summary</b> tab. The default is the <b>past 12 hours</b> .
<b>Auto-refresh rate</b>	Determines the rate at which the <b>Home</b> page and <b>Monitors</b> page > <b>Summary</b> tab automatically refresh. The default setting is to refresh every 15 minutes.
<b>Notifications</b>	Determines which notifications are included in the unacknowledged notifications count on the <b>Home</b> page. The default is to see all notifications, regardless of who created them. If you select <b>Only show my notifications</b> , the <b>Home</b> page count includes only the notifications that you created but have not acknowledged. This option is available only to system administrators. Domain administrators and limited administrators always see only the notifications that they have created, but have not acknowledged.
<b>Virus and Risks Activity Summary display</b>	Determines how the <b>Virus and Risks Activity Summary</b> on the <b>Home</b> page displays data.

## Preferences: Security Status

You can use the **Security Status** tab to change the default options that are used for the security status thresholds. These thresholds determine when the **Home** page **Security Status** on the console turns red to indicate that something needs your attention.

The default for most options is 10 percent and 30 days.

## Preferences: Logs and Reports

You can use the **Logs and Reports** tab to change the options that are used for logs and report displays. You can also configure legacy logs to be uploaded to the server.

**Table 389: Options for logs and reports**

Option	Description
<b>Date format</b>	Specifies the date format that is used when dates are displayed in reports and logs on the console or in a browser. The default is <b>MMDDYY</b> .  <b>Note:</b> This setting does not apply to virus definitions dates and the versions that are displayed in tables, which always use a Y-M-D format.
<b>Date separator</b>	Specifies the type of separator that is used when dates are displayed in reports and logs on the console or in a browser. The default setting is a forward slash (/).
<b>Maximum number of rows in report table</b>	Specifies the maximum number of rows that are displayed in table-style HTML reports. The default setting is 200 rows; the maximum possible number of rows is 99,999 rows.
<b>Time zone used in export</b>	Specifies the time zone that is used when you export logs to other computers.
<b>Subnet format for IPv4 to group by</b>	Specifies the IP address subnet format that you want to use to group information in log and report displays. You can choose the <b>Class B</b> , the <b>Class C</b> , or a <b>Custom</b> subnet format.



Option	Description
<b>Custom subnet format for IPv4</b>	If you select <b>Custom</b> for <b>Subnet format to group by</b> , specifies the custom subnet mask that you want to use to group information in log and report displays. You can use the dot-decimal notation xxx.xxx.xxx.xxx, where each of the triplets is a decimal number in the range 0 to 255, inclusive.
<b>Subnet format for IPv6 (CIDR prefix)</b>	Insert the IPv6 CIDR subnet prefix that is appropriate for your environment.
<b>Include filter settings in report</b>	Specifies whether the query criteria that are used to generate a report appear in the report. The default setting is not to include the filter settings.

## Command Status

You can use this tab to view the status of the commands that you have issued from the console and their details. This tab displays the commands that you have run on clients from the console, not actions such as adding a risk to an Exceptions policy.

Also, you can use this tab to cancel a scan. A cancel icon displays in the **Command** column of any scan that is in progress. You can click the cancel icon to cancel a scan that is in progress.

You can select a command, and then you can click **Details** to display more information about any command in the table. If the command was sent to multiple computers, you can get separate details for each computer.

### NOTE

The Command Status log shows a report icon in the **Completion** column that you can click to get more details about scan detections. The details view also includes an icon so that you can drill down for details by computer.

### [Command Status: Details](#)

Also, you can view the command progress of the selected command. The pie chart shows the status of all commands.

**Table 390: Filter options to view command status**

Option	Description
<b>Show commands</b>	Determines the time range of the commands that you view the status of. For example, you can select <b>Issued at any time</b> to view all the commands of a particular type that have run. Or you can view the commands that have been issued in the last seven days.
<b>of type</b>	Determines which type of command you view the detailed status of, such as the <b>Update Content</b> command or <b>Enable Auto-Protect</b> command. <a href="#">What are the commands that you can run on client computers?</a>
<b>with status:</b>	Determines the status of the commands that you view the detailed status of, such as <b>Received</b> , <b>Completed</b> , or <b>Canceled</b> .

**Table 391: Command Status table information**

Column name	Description
<b>Time Issued</b>	The date and time at which the command was invoked.
<b>Issued By</b>	The name of the administrator who invoked the command.
<b>Command</b>	The name of the command that you issued.
<b>Description</b>	A description of the command.
<b>Clients Affected</b>	The number of clients that the command affected.

Column name	Description
<b>Completion Status</b>	The percentage complete for the command.
<b>Source</b>	The source of the command.
<b>Source IP address</b>	The source IP address of the command.

## Command Status: Details

The **Command Status Details** view displays the details of a particular command in a secondary window.

[Command Status Details filter settings](#)

**Table 392: Command Status Details log columns**

Column name	Description
<b>Begin Time</b>	The date and time at which the command was invoked.
<b>Last Update</b>	The date and time of the last update that the client sent to the server about this command.
<b>Computer/IP Address</b>	The name and the IP address of the computer on which the command was executed.
<b>User</b>	If a user was logged on the computer at the time the command was invoked, the user's logon name.
<b>Domain</b>	The name of the domain in which the command was executed.
<b>Status</b>	The status of the command, such as <b>Not received</b> or <b>In progress</b> .
<b>Details</b>	<p>The <b>Details</b> column contains more information about the command's status. It contains one of the following statements:</p> <ul style="list-style-type: none"> <li>• <b>Success</b></li> <li>• <b>Client did not execute the command</b></li> <li>• <b>Client did not report any status</b></li> <li>• <b>Command was a duplicate and not executed</b></li> <li>• <b>Spoiled command could not restart</b></li> <li>• <b>Security risk found</b></li> <li>• <b>Scan was suspended</b></li> <li>• <b>Scan was aborted</b></li> <li>• <b>Scan did not return status</b></li> <li>• <b>Scan failed to start</b></li> <li>• <b>Auto-Protect could not be turned on</b></li> <li>• <b>LiveUpdate download is in progress</b></li> <li>• <b>LiveUpdate download failed</b></li> <li>• <b>Quarantine delete failed</b></li> <li>• <b>Quarantine delete partial success</b></li> </ul> <p>You can click the link to view a report that shows the associated entries in the <b>Risk</b> log. All the <b>Risk</b> logs associated with that command's status may not be immediately available to the <b>Details</b> view. Status may be uploaded and processed at different rates, so a time lag may take place for some commands.</p>
<b>Supplementary Details</b>	<p>A description of the status of the command from the client.</p> <p><b>Note:</b> No additional information is available for some commands. If no additional information is available, this column is blank.</p>

**Table 393: Command Status Details filter settings**

Option	Description
<b>Use a saved filter</b>	Specifies to use a saved filter to view command status entries. The default is <b>Default</b> .
<b>Computer</b>	Specifies to filter the command status entries by the computer name. The default is <b>*</b> .
<b>Status</b>	Specifies to filter the command status entries by the status. The default is <b>All</b> .
<b>Details</b>	Specifies to filter the command status entries by the details. The default is <b>All</b> .
<b>Limit</b>	Specifies the limit for the number of entries that appear in the <b>Command Status</b> window. The default is <b>20 entries</b> .

## Scheduled Reports

You can configure the reports that run automatically based on the schedule that you want. Scheduled reports are emailed to recipients at the scheduled interval, so you must include the email address of at least one recipient.

**The following reports are available only as scheduled reports:**

- **Client Software Rollout (Snapshots)**
- **Clients Online/Offline Over Time (Snapshots)**
- **Clients With Latest Policy over Time (Snapshots)**
- **Non-Compliant Clients Over Time (Snapshots)**
- **Virus Definition Rollout (Snapshots)**

By default, you see all the reports that you have scheduled, regardless of type. You can use the **Show report type** list box to filter the view to see the scheduled reports of a specific type.

When you first create a scheduled report, you must use a default filter or a filter that you have already saved. After you have created and configured a scheduled report, then you can use **Edit filter** link to change the report's content. You can use the **Edit** link to change the configuration settings that determine the schedule, email recipients, and report type details.

**Table 394: Scheduled Reports options**

Option	Description
<b>Add</b>	Adds a new scheduled report and configure its schedule options. <a href="#">Scheduled Reports: Add Scheduled Report or Edit Scheduled Report</a>
<b>Edit</b>	Edits the schedule and the email configuration options for the selected scheduled report. <a href="#">Scheduled Reports: Add Scheduled Report or Edit Scheduled Report</a>
<b>Edit Filter</b>	Edits the filter that is used for the selected scheduled report. <a href="#">Scheduled Reports: Edit Filter</a>
<b>Delete</b>	Deletes the selected scheduled report.
<b>Show report type</b>	Filters the list of scheduled reports to show only the selected type. By default, the list displays all types of reports.

**Table 395: Scheduled Reports list columns**

Column name	Description
<b>Report Name</b>	The name that is assigned to the report.
<b>Report Title / Report Type</b>	The report title and report type.
<b>Filter</b>	The filter that is assigned to the report.
<b>Schedule / Last Run</b>	The schedule for the report, and the date and the time that the report was last generated.
<b>Send To</b>	The recipients of the report.
<b>Created By</b>	The name of the administrator who created the report.

## Scheduled Reports: Add Scheduled Report or Edit Scheduled Report

Use this dialog box to add a new scheduled report or to edit an existing scheduled report.

**Table 396: Scheduled report configuration options**

Option	Description
<b>Report name</b>	Identifies this scheduled report.
<b>Description</b>	Describes this scheduled report and the information in it for later reference.
<b>Enable this scheduled report</b>	Specifies to run this report on the schedule you configured. This option is enabled by default.
<b>Report type</b>	Specifies the type of report that you want to schedule. <a href="#">About the types of Symantec Endpoint Protection Manager reports</a>
<b>Select a report</b>	In the <b>Select a report</b> list box, select the name of the report that you want to schedule. The options available for selection are specific to the <b>Report type</b> selected.
<b>Use a saved filter</b>	Specifies a saved filter configuration that you want to use or use the default configuration. When you associate a saved filter with a scheduled report, make sure that the filter does not contain custom dates. If the filter specifies a custom date, you get the same report every time the report runs.
<b>Run every</b>	Specifies the frequency with which this report should be emailed to recipients. You can select one interval from hours, days, weeks, and months. The data that is used in scheduled reports is updated in the database every hour. The report is emailed to recipients at the hour and the time interval that you set by using this option. At the time that Symantec Endpoint Protection emails the report, the data is current to within one hour.
<b>Start after</b>	Specifies the date (MM/DD/YY) and the time of day (hour and minutes) when the report next runs.
<b>Send this report to System Administrators</b>	Sends this report to the email address for each administrator. The data is taken from the database at the time set and is emailed to system administrators as an .mht file attachment. You must already have set up mail server properties for email notifications to work.
<b>Send this report to the following comma-separated email addresses</b>	Specifies the person or a list of people that you want this report to be sent to. The data is taken from the database at the time set and is emailed to these recipients as an .mht file attachment. You must already have set up mail server properties for email notifications to work.

[How to run scheduled reports](#)

---

## Scheduled Reports: Edit Filter

Use this dialog box to change the filter settings that are used for a scheduled report that you configured previously. The filter options that are available depend on the type of report that you scheduled. They are the same as the Basic Settings and Additional Settings for each type of quick report filter.

You can click **Tell me more** at the top of the **Edit Filter** dialog box to see context-sensitive help for each filter option.

## Virus and Spyware Protection

### Auto-Protect: Notifications

You can set notification options for Auto-Protect detections.

Notification messages for the client for Mac appear in the macOS (or Mac OS X) Notification Center. Due to the character limitations of Notification Center, you cannot customize the messages for Mac.

#### NOTE

A lock icon appears next to some options. Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

**Table 397: Notification options**

Option	Description
<b>Display a notification message on the infected computer</b>	You can lock or unlock this option to prevent or allow user changes. Enables or disables displaying notification messages on infected computers when Auto-Protect finds a virus or a security risk. When this option is enabled, you can modify the type of information that you want to appear in the notification.
<b>Display the Auto-Protect results dialog on the infected computer</b>	You can lock or unlock this option to prevent or allow user changes. Enables or disables displaying Auto-Protect results on infected computers.

**Table 398: Notification message fields**

Label	Field	Description
<b>Scan type</b>	<b>LoggedBy</b>	The type of scan that detected the virus or security risk.
<b>Event</b>	<b>Event</b>	The type of event, such as "Risk Found."
<b>Security risk detected</b>	<b>SecurityRiskName</b>	The name of the virus or security risk that was found.
<b>File reputation</b>	<b>FileReputation</b>	For Download Insight detections, this field indicates the trustworthiness of the file based on information that Symantec has collected. The information includes how long Symantec has known about the file, and how many users use the file.
<b>File</b>	<b>PathAndFilename</b>	The complete path and name of the file that the virus or the security risk has infected.
<b>Location</b>	<b>Location</b>	The drive on the computer on which the virus or security risk was located.
<b>Computer</b>	<b>Computer</b>	The name of the computer on which the virus or security risk was found.

Label	Field	Description
User	User	The name of the user who was logged on when the virus or security risk occurred.
Action taken	ActionTaken	The action that was taken in response to detecting the virus or security risk. This action can be either the first action or second action that was configured.
Date found	DateFound	The date on which the virus or security risk was found.

[The types of security policies](#)

## Internet Email Auto-Protect: Notifications

For client versions earlier than 14.2 RU1, you can configure notifications options for Auto-Protect scans of Internet email. You can configure the information that you want to include in notifications. This information includes to whom email notification messages should be sent, and whether or not to display progress indicators on client computers.

### NOTE

A lock icon appears next to some options. Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

**Table 399: Notifications options**

Option	Description
<b>Notifications</b>	<p>Enables or disables the display of notification messages on infected computers</p> <p><b>The following option is available:</b></p> <ul style="list-style-type: none"> <li>• <b>Display a notification message on the infected computer</b> When this option is enabled, you can modify the information that should appear when Auto-Protect finds a virus or a security risk. This option is enabled by default.</li> </ul>
<b>Email Notifications</b>	<p>Enables or disables the notifications about infected email</p> <p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Insert a warning into the email message:</b> Adds an email warning to infected messages. This option is enabled by default. Click <b>Warning</b> to change the text. <a href="#">Insert Warning</a></li> <li>• <b>Send email to the sender:</b> Notifies the senders of infected messages in Internet email applications. This option is disabled by default. When this option is enabled, you can click <b>Sender</b> to change the default text. <a href="#">Email Server</a> <a href="#">Message</a></li> <li>• <b>Send email to others:</b> Notifies the specified recipients of infected messages in email applications. This option is disabled by default. When this option is enabled, you can click <b>Others</b> to change the default text. <a href="#">Send Email to Others: Others</a></li> </ul>

Option	Description
<b>Progress Notifications</b>	<p>Enables or disables the display of a progress message and an icon on client computers during email scans</p> <p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Display a progress indicator when email is being sent.</b> This option is disabled by default.</li> <li>• <b>Display a notification area icon.</b> This option is disabled by default.</li> </ul>

**Table 400: Notification message fields**

Label	Field	Description
<b>Scan type</b>	<b>LoggedBy</b>	The type of scan, such as on-demand or scheduled, that detected the virus or security risk.
<b>Event</b>	<b>Event</b>	The type of event, such as "Risk Found."
<b>Security risk detected</b>	<b>SecurityRiskName</b>	The name of the virus or security risk that was found.
<b>File reputation</b>	<b>FileReputation</b>	For Download Insight detections, this field indicates the trustworthiness of the file based on information that Symantec has collected. The information includes how long Symantec has known about the file, and how many users use the file.
<b>File</b>	<b>PathAndFilename</b>	The complete path and name of the file that the virus or the security risk has infected.
<b>Location</b>	<b>Location</b>	The drive on the computer on which the virus or security risk was located.
<b>Computer</b>	<b>Computer</b>	The name of the computer on which the virus or security risk was found.
<b>User</b>	<b>User</b>	The name of the user who was logged on when the virus or security risk occurred.
<b>Action taken</b>	<b>ActionTaken</b>	The action that was taken in response to detecting the virus or security risk. This action can be either the first action or second action that was configured.
<b>Date found</b>	<b>DateFound</b>	The date on which the virus or security risk was found.

[The types of security policies](#)

## Microsoft Outlook or Lotus Notes Auto-Protect: Notifications

You can configure notifications options for Auto-Protect scans of Microsoft Outlook. You can configure the information that should appear in notifications.

For client versions earlier than 14.2 RU1, you can also configure these settings for Auto-Protect for Lotus Notes.

### NOTE

A lock icon appears next to some options. Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

**Table 401: Notifications options**

Group: Option	Description
<b>Notifications</b>	<p><b>Display a notification message on the infected computer</b></p> <p>Enables or disables the display of a notification message on an infected computer when Auto-Protect finds a security risk.</p> <p>When this option is enabled, you can modify the type of information that you want to appear on the affected computer.</p>
<b>Email Notifications</b>	<p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Insert a warning into the email message</b> Adds an email warning to an infected message. You can click <b>Warning</b> to change the default text. <a href="#">Insert Warning</a></li> <li>• <b>Send email to sender</b> Notifies the senders of infected messages in Internet email applications. You can click <b>Sender</b> to change the default text. <a href="#">Email Server Message</a></li> <li>• <b>Send email to others</b> Notifies the specified recipients of infected messages in email applications. You can click <b>Others</b> to change the default text and to specify recipients. <a href="#">Send Email to Others: Others</a></li> </ul>

**Table 402: Notification message fields**

Label	Field	Description
<b>Scan type</b>	<b>LoggedBy</b>	The type of scan, on-demand, scheduled, and so on, that detected the virus or security risk.
<b>Event</b>	<b>Event</b>	The type of event, such as "Risk Found."
<b>Security risk detected</b>	<b>SecurityRiskName</b>	The name of the virus or security risk that was found.
<b>File reputation</b>	<b>FileReputation</b>	For Download Insight detections, this field indicates the trustworthiness of the file based on information that Symantec has collected. The information includes how long Symantec has known about the file, and how many users use the file.
<b>File</b>	<b>PathAndFilename</b>	The complete path and name of the file that the virus or the security risk has infected.
<b>Location</b>	<b>Location</b>	The drive on the computer on which the virus or security risk was located.
<b>Computer</b>	<b>Computer</b>	The name of the computer on which the virus or security risk was found.
<b>User</b>	<b>User</b>	The name of the user who was logged on when the virus or security risk occurred.
<b>Action taken</b>	<b>ActionTaken</b>	The action that was taken in response to detecting the virus or security risk. This action can be either the first action or second action that was configured.
<b>Date found</b>	<b>DateFound</b>	The date on which the virus or security risk was found.

## [The types of security policies](#)

## Rules: Notifications

You can enable or disable the notifications that appear on the client when a firewall rule blocks an application or service on the client computer. You can customize the text for this type of notification as well as notifications that appear on the client computer when the following events occur:



- Applications on the client try to access the network.
- Applications that normally access the network are upgraded.
- The client software is updated.

**Table 403: Notifications tab options**

Option	Description
<b>Display notification on the computer when the client blocks an application</b>	Displays a standard message on the client when the client blocks an application. You specify which applications to block on the <b>Rules</b> tab.
<b>Set Additional Text</b> (Windows only)	Adds customized text to the bottom of the standard message.
<b>Additional text to display if the action for a firewall rule is 'Ask'</b> (Windows only)	Displays a standard message on the client every time an application asks the user whether to access the network. You cannot enable or disable these messages; you can only add custom text to the standard text.  <b>Note:</b> The amount of text that can be displayed in this notification on a client computer is limited by the operating system. To avoid the truncation of the notification text, you should limit your added text to no more than 120 characters.

## Monitors: Notifications

You can use the Notifications tab for the following tasks:

- To view the list of notifications that you create, and to acknowledge notifications.
- To access the dialog boxes where you create new notifications and modify existing notification filters and schedule options.  
[Notification Conditions](#)

**Table 404: Basic Settings for the Notifications log filter**

Option	Description
<b>Use a saved filter</b>	Specifies the filter that you want to use to create the log view. You can use the default filter or a custom filter that you have named and saved for viewing notification information.
<b>Time range</b>	Specifies the time range of events you want to view from the log. If you select <b>Set specific dates</b> , additional date-setting options appear.
<b>Start date</b>	Specifies the start date for the time range that you want to view information about. Available only when you select <b>Set specific dates</b> for the time range.
<b>End date</b>	Specifies the end date for the time range that you want to view information about. Available only when you select <b>Set specific dates</b> for the time range.
<b>Additional Settings</b>	Displays the additional configuration options that are available for the notifications log view. Click <b>Additional Settings</b> and <b>Basic Settings</b> to toggle back and forth between them.
<b>Save Filter</b>	Save the filter settings under a name for future use.
<b>Notification Conditions</b>	Displays a page with the settings to configure to create a new notification condition, or to edit an existing condition.
<b>View Notifications</b>	Displays the <b>Notifications</b> log filtered by the current filter settings.

**Table 405: Additional filter settings for the Notifications log view**

Option	Description
<b>Acknowledged status</b>	Specifies whether the Notifications log view shows all notifications, the notifications that have been acknowledged, or the notifications that have not been acknowledged.
<b>Notification type</b>	Specifies the type of notification condition that you want to view information about. You can specify a particular notification condition or view all of them.
<b>Created by</b>	You can specify notification conditions created by a particular user or by all users.
<b>Notification name</b>	Specifies the name of a particular notification condition that you want to view information about. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters. You can also click the ellipsis to select from a list of notification condition names. By default, all notification conditions that have been created are included.
<b>Limit</b>	Specifies how many entries to display on each page of the view.

## Add or Edit Notification Condition

You can use this page to configure notification conditions.

**You can configure the following types of notification actions to occur:**

- Log entries to the database.
- Run a batch file or other executable file when triggered by the notification.
- Send email to administrators or other individuals.

These notifications are used primarily to notify administrators, although you can configure a notification email to be sent to anyone with a valid email address.

### NOTE

To send email notifications, you must also configure a mail server. You can configure a mail server by using the **Email Server** tab on the **Admin > Servers** page.

Not all filter options are available for all types of notifications.

**Table 406: Possible filter options when you create a notification**

Option	Description
<b>Notification name</b>	Specifies a name to distinguish the notification that you add.
<b>Domain</b>	Specifies the domain in which you want the conditions that you set to trigger the notification. This field accepts a comma-separated list as input. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters. You can also click the dots to select from a list of known domains.
<b>Group</b>	<p>Specifies the group in which you want the conditions that you set to trigger the notification. This field accepts a comma-separated list as input. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters. You can also click the dots to select from a list of known groups.</p> <p><b>Note:</b> All groups are subgroups of the default parent group. When this filter searches for groups, it searches hierarchically starting with the name of the default group. Unless the name of your group starts with the same letter, you should precede the search string with an asterisk when using wildcards.</p> <p><b>Note:</b> For example, if you have a group named Purchasing, and you type p* into this box, no group is found and used in the view. To find a group named Purchasing, you need to use *p* instead.</p>

Option	Description
<b>Server</b>	Specifies the server that you want to trigger a notification. If you set multiple servers to trigger a notification, you may get many notifications for each event. This field accepts a comma-separated list as input. You can use the wildcard character question mark (?), which matches any one character, and the asterisk (*), which matches any string of characters. You can also click the dots to select from a list of known servers.
<b>Computer</b>	Specifies the computer in which you want the conditions that you set to trigger the notification. You can use the asterisk (*) wildcard character, which matches any string of characters. This field also accepts a comma-separated list as input.
<b>Risk name</b>	Specifies the name of the risk that you want to trigger a notification. You can use the asterisk (*) wildcard character, which matches any string of characters. This field also accepts a comma-separated list as input.
<b>Application name</b>	Specifies the name of the application on the watchlist that you want to trigger a notification. The asterisk (*) wildcard character is accepted. For multiple entries, you can use a comma-delimited list.

**Table 407: Notification conditions options**

Option	Description
<b>Outbreak type</b>	For <b>Client security alert</b> and <b>Risk outbreak</b> , specifies the type and extent of the outbreak that should trigger this notification. <b>The outbreak type that you select results in the following information:</b> <ul style="list-style-type: none"> <li>• <b>Occurrences on any computer</b> The number of security events or risks that are found in the number of minutes that you set.</li> <li>• <b>Occurrences on single computer</b> The number of security events or risks that are found on computer name in the number of minutes that you set.</li> <li>• <b>Occurrences on distinct computers</b> The number of attacked computers or infected computers that are found in the number of minutes that you set.</li> </ul> <b>Note:</b> In this context, infected means that a risk was detected. It does not necessarily mean that the risk is still active.
<b>Failure Type</b>	For <b>Authentication failure</b> , specifies the extent of the failure that should trigger this notification. You can choose to have a notification triggered when an occurrence takes place on any server or on a single server.
<b>Compliance events</b>	For <b>Client security alert</b> , specifies that a compliance-related event, such as a Host Integrity failure, should trigger this notification.
<b>Network and Host Exploit Mitigation events</b>	For <b>Client security alert</b> , specifies that a firewall activity or Intrusion or Memory Exploit Mitigation activity should trigger this notification. These activities indicate the detection of anomalous network activity patterns. Anomalous network activity patterns include events such as denial-of-service attacks, port scans, and other activities that the Intrusion Prevention signatures identify. To notify you when a traffic event matches a firewall rule criteria, you must configure a client security event for firewall activity. Configuring a client security event for firewall activity enables the <b>Send Email Alert</b> option in the <b>Logging</b> column of the <b>Rules</b> list.
<b>New software package event</b>	Specifies that a notification is triggered when a new client package is installed, or when new security definitions are installed. You must specify at least one kind of package, but you can specify both.
<b>Packet events</b>	For <b>Client security alert</b> , specifies that a Packet log entry should trigger this notification.

Option	Description
<b>Device Control events</b>	For <b>Client security alert</b> , specifies that a device manager-related event should trigger this notification. For example, Symantec Endpoint Protection blocked a device from connecting to the network. <b>Note:</b> You must have checked <b>Log blocked devices</b> under <b>Device Control</b> in the <b>Application and Device Control Policy</b> for this server-side notification to be sent successfully.
<b>Traffic events</b>	For <b>Client security alert</b> , specifies that a firewall rule violation should trigger this notification.
<b>Application Control events</b>	For <b>Client security alert</b> , specifies that an application event should trigger this notification. <b>Note:</b> You must have checked <b>Enable logging</b> and <b>Send Email Alert</b> on the <b>Action</b> tab for an application control rule condition in the <b>Application and Device Control Policy</b> for this server-side notification to be sent successfully.
<b>Server activity</b>	For <b>System event</b> , specifies that a server-related event should trigger this notification. <b>For example, this option can include the following events:</b> <ul style="list-style-type: none"> <li>• Server startup and shutdown</li> <li>• The creation of a new client installation package</li> <li>• Import events</li> <li>• A database log sweep</li> <li>• Remote client installation success</li> <li>• LiveUpdate success</li> <li>• Unmanaged computer search completion</li> <li>• The removal of clients that have not checked in within the configured interval</li> <li>• The importation of an Organizational Unit from Active Directory</li> </ul>
<b>Replication failure</b>	For <b>System event</b> , specifies that a replication failure should trigger this notification.
<b>System error</b>	For <b>System event</b> , specifies that a server error should trigger this notification. <b>For example, this option can include the following events:</b> <ul style="list-style-type: none"> <li>• Server startup failure</li> <li>• LiveUpdate failure</li> <li>• Remote client installation failure</li> <li>• A scheduled report failure</li> <li>• Unmanaged computer search failure</li> </ul>
<b>Severity</b>	For <b>System event</b> , specifies the severity level of the problem that should trigger this notification.
<b>Damper</b>	Specifies the length of the damper period, in minutes or hours, that you want to use for this notification. Some logs use a damper period for event aggregation. Events are held on the clients for the damper period before they are aggregated into a single event and then uploaded to the console. The damper period helps to reduce events to a manageable number. The default damper setting is Auto (automatic). If a notification is triggered and the trigger condition continues to exist, the notification action that you configured is not performed again for 60 minutes. For example, suppose you configure a notification to alert you when a virus infects five computers within one hour. If a virus continues to infect your computers at or above this rate, you receive notifications every hour. The notifications continue until the rate slows to fewer than five computers per hour. For <b>Network load alert: requests for Virus and Spyware full definitions</b> , the requests log only on the server, not on the client, and the default damper is 5 hours. If you set the <b>Damper</b> period to <b>None</b> for notifications about critical events, you should make sure that clients can upload critical events immediately. The relevant notifications include the following: <b>Client security alert</b> , <b>Single risk event</b> , <b>New risk detected</b> , and <b>Risk outbreak</b> . The <b>Let clients upload critical events immediately</b> option is enabled by default and configured in the <b>Communications Settings</b> dialog box.
<b>Scan type</b>	Specifies the type of scan that should trigger this notification. This option applies only to <b>New risk detected</b> , <b>Risk outbreak</b> , and <b>Single risk event</b> .

Option	Description
<b>Action taken</b>	<p>Specifies the configured action that you want to trigger this notification.  This option applies only to <b>New risk detected</b>, <b>Risk outbreak</b>, and <b>Single risk event</b>.  <b>You can select one of the following:</b></p> <ul style="list-style-type: none"> <li>• <b>All</b></li> <li>• <b>Access denied</b>  Specifies the events where Auto-Protect prevented a file from being created.</li> <li>• <b>Action invalid</b>  Specifies the events where the remediation action was invalid. These risks may still be present on the computer.</li> <li>• <b>All actions failed</b>  Specifies the events where both the primary action and the secondary action that were configured for the risk cannot be carried out. These risks are still present on the computer.</li> <li>• <b>Cleaned</b>  Specifies the events where the software cleaned a virus from the computer.</li> <li>• <b>Cleaned by deletion</b>  Specifies the events where the action configured was Clean, but a file was deleted because that was the only way it can be cleaned. For example, this action is generally needed for Trojan horse programs.</li> <li>• <b>Cleaned or macros deleted</b>  Specifies the events where a macro virus was cleaned from a file either by deletion or some other means. This action applies only to the events that have been received from the computers that run Symantec AntiVirus 8.x or earlier versions.</li> <li>• <b>Deleted</b>  Specifies the events where Symantec Endpoint Protection deleted an object, such as a file or a registry key, to remove a risk.</li> <li>• <b>Excluded</b>  Specifies the events where users chose to exclude a security risk from detection.</li> <li>• <b>Left alone</b>  Specifies the events where a risk was left alone. This action can occur if the first configured action is Leave alone. This action can also occur if the second configured action is Leave alone and the first configured action is not successful. This action may mean that a risk is active on the computer.</li> <li>• <b>No repair available</b>  Specifies the events where a risk was detected but no repair is available for the side effects of this risk.</li> <li>• <b>Partially repaired</b>  Specifies the events where Symantec Endpoint Protection cannot completely repair the effects of a virus or security risk.</li> <li>• <b>Pending repair</b>  Specifies the events where a user still needs to take action to complete the remediation of a risk on a computer. For example, this action may occur if a user hasn't responded to a prompt to terminate a process.</li> <li>• <b>Process terminated</b>  Specifies the events where a process had to be terminated on a computer to mitigate a risk.</li> <li>• <b>Process termination pending restart</b>  Specifies the events where a computer needs to be restarted to terminate a process to mitigate a risk.</li> <li>• <b>Quarantined</b>  Specifies the events where Symantec Endpoint Protection quarantined a virus or a security risk.</li> <li>• <b>Suspicious</b>  Specifies the events where SONAR scan detected a potential risk but has not remediated it. Symantec Endpoint Protection did not remediate the risk either because it cannot or because you have configured it to only log detections.</li> </ul>

Option	Description
<b>Notification condition</b>	<p>For <b>Authentication failure</b>, <b>Risk outbreak</b>, and <b>Client security alert</b> notifications, specifies the number of events that must occur within this number of minutes to trigger a notification.</p> <p>For <b>Network load alert: requests for Virus and Spyware full definitions</b>, specifies the number of requests for full definitions that must occur within this number of minutes to trigger a notification.</p> <p><b>For a Virus definitions out-of-date notification, specifies that the following conditions trigger a notification:</b></p> <ul style="list-style-type: none"> <li>The number of days that definitions must be out-of-date</li> <li>The number of computers that must have virus definitions that are older than this value</li> </ul> <p>For <b>Low Bandwidth Definitions Out-of-date</b>, specifies the number of computers that report that they have definitions older than this number of days.</p>
<b>Include only clients that have checked in with the management server today</b>	For a <b>Virus definitions out-of-date</b> notification, specifies that only the clients that have checked in with their server on or after midnight today should trigger this notification.

The following table describes the actions that you can configure to take place when a notification is triggered.

**Table 408: Action options for notifications**

Option	Description
<b>Log the notification</b>	Specifies that the notification be written to the database.
<b>Run the batch or executable file</b>	Specifies that the notification causes a batch or an executable file to run. You can type the name of the file in the text box.
<b>Send email to system administrators</b>	Specifies that the notification be sent in an email to all system administrators.
<b>Send email to</b>	Specifies that the notification be in the form of an email to one or more addresses. You can type multiple email addresses separated by commas or semicolons. Spaces are not allowed.
<b>Email subject</b>	Specifies a customized email subject.
<b>Report type</b>	<p>Specifies the content of the email notification.</p> <p>This option is only available for the <b>Client security alert</b>, <b>New risk detected</b>, <b>Risk outbreak</b>, and <b>Virus definitions out-of-date</b> notification conditions.</p> <p><b>Note:</b> This option is ignored when the action is to run a batch file or executable file.</p> <p><b>You can select one of the following to be included in the email notification:</b></p> <ul style="list-style-type: none"> <li><b>Summary report</b> A report that summarizes the activity that triggered the notification</li> <li><b>Event list</b> The event list that triggered the notification</li> </ul> <p><b>Note:</b> This notification differs from scheduled reports, which are delivered as email attachments.</p>

## Notification Conditions

Use this page to view notifications, add a notification condition, or to modify or delete a condition that already exists. Notifications are triggered when certain security-related conditions are met. The notification can take the form of a log entry or an email, or it can run a batch file or other executable file.

Some notifications are enabled by default when you install Symantec Endpoint Protection Manager. For example, the **Risk Outbreak**, **Server Health**, and **Power Eraser Recommended** notifications are enabled by default. You can enable other types of preconfigured notifications, such as **New risk detected** or **Single risk event**. You can edit and customize any of the notifications.

Use the **Show notification type** option to filter the display. You only see the notification conditions that match the type that is selected in this list box. If you want to see all types of notification conditions, you must select **All**.

#### NOTE

If the type of notification condition that you created is not selected in the **Show notification type** list box, you do not see the new notification condition. To see your new notification condition, you must select **All** or the same type of condition that you created in this list.

## Global Scan Options: Scan Network Drive: Change password

Changes the password for scans of mapped network drives. The default password is symantec.

## Miscellaneous

The Windows Security Center (WSC) monitors the security status of the computer. The Windows Security Center provides alerts on your client computers if any security software is out of date or if security settings should be strengthened.

You can configure all the Windows Security Center options on your client computers that run Windows XP SP3 only. You can only configure the **Display a Windows Security Center message when definitions are outdated** option for Windows Vista and Windows 7 and later. Windows Security Center was renamed as Action Center in Windows 7/8, and renamed as Security and Maintenance in Windows 10.

The Windows Security Center was renamed as the Action Center in Windows 7/8 and as Security and Maintenance in Windows 10.

**Table 409: Miscellaneous options**

Option	Description
<b>Disable Windows Security Center</b>	<p>Specifies when to disable Windows Security Center on the clients that run Windows XP SP3.</p> <ul style="list-style-type: none"><li>• <b>Never</b> Never disable Windows Security Center. Leave it completely alone. This setting is the default value.</li><li>• <b>Once</b> Disable Windows Security Center only one time. If a user re-enables it, the client does not disable it again.</li><li>• <b>Always</b> Always disable Windows Security Center. If a user re-enables it, it is disabled again immediately.</li><li>• <b>Restore</b> Re-enable Windows Security Center only if the client disabled it.</li></ul> <p><b>Note:</b> Symantec product status is always available in Symantec Endpoint Protection, regardless of whether Windows Security Center is enabled or disabled.</p>
<b>Display antivirus alerts within Windows Security Center</b>	<p>Specifies when Windows Security Center displays antivirus alerts.</p> <p><b>Select one of the following:</b></p> <ul style="list-style-type: none"><li>• <b>Enable</b> Windows Security Center displays these alerts in the notification area.</li><li>• <b>Disable</b> Windows Security Center does not display these alerts on the notification area.</li><li>• <b>Use existing setting</b> Windows Security Center uses the existing setting for displaying these alerts.</li></ul>

Option	Description
<b>Display Windows Security Center message when definitions are outdated. Warn after x days</b>	<p>Set the time period after which Windows Security Center considers definitions files to be out of date and displays a message about it.</p> <p>Specifies the number of days that definitions are allowed to be out of date.</p> <p>The value must be in the range from 1 to 30.</p> <p>The client checks every 15 minutes to compare the out-of-date time, the date of the definitions, and the current date. Typically, no out-of-date status is reported to Windows Security Center because definitions are usually updated automatically. If you update definitions manually, you might wait up to 15 minutes to view an accurate status.</p>
<b>Coexist with Windows Defender</b>	<p>This option is available in 14.3 RU1 and 14.3 RU1 MP1 only. In 14.3 RU2, this option was removed from the user interface.</p> <p>When Windows Defender and Symantec Endpoint Protection are both enabled and running on the same computer, the Auto-Protect scan runs after Windows Defender. Auto-Protect can detect any threats that Windows Defender misses.</p> <p>If Windows Defender is disabled on the client computers, you should disable this option. Otherwise, Auto-Protect continues to run in a delayed state.</p> <p>Auto-Protect cannot run in coexistence mode on an endpoint that is protected by a File Based Write Filter (FBWF). These endpoints ignore this option.</p>
<b>Internet Browser Protection</b>	<p>Specifies a URL that points to the Symantec Support website or to a custom URL to use as the home page when a security risk takes over a client computer's home page. The client uses this URL when it repairs the risk.</p> <p>The URL also appears in the System event log for the client on which the error occurs.</p>

## Miscellaneous: Log handling

You can use this tab to set the options that are related to virus and spyware logs.

### NOTE

Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

**Table 410: Virus and spyware log handling options**

Options	Description
<b>Show</b>	<p>Specifies the category of events you want to display. Select from the following categories, and then check the events that you want the client to send to the management server.</p> <ul style="list-style-type: none"> <li>• <b>All virus and spyware protection events</b></li> <li>• <b>Scanning and infection events</b></li> <li>• <b>Virus definition events</b></li> <li>• <b>Management and configuration events</b> (Windows only)</li> <li>• <b>Startup and shutdown events</b></li> </ul> <p>By default, clients always send certain types of events to the management server (such as <b>Scan stopped</b> or <b>Scan started</b>). You can choose to send or not send other types of events.</p>
<b>Delete logs older than</b>	<p>Specifies the number of days you want to keep antivirus-related events in the logs.</p> <p>The option does not affect any events that the clients send to the management console. You can use the option to reduce the actual log size on the client computers.</p>



Options	Description
<b>Aggregate events for</b>	<p>Specifies the number of minutes that the client computer aggregates identical virus and spyware events before it forwards the aggregated event to the management server.</p> <p>Symantec Endpoint Protection aggregates virus and spyware events to keep the number of events manageable. At the first occurrence of an event, the aggregation period begins and subsequent identical events are aggregated until the aggregation period expires. The client always sends the first occurrence of an event to the management server at the next heartbeat. The client then sends the aggregated event at the next heartbeat after the aggregation period expires. If the aggregation period is longer than the heartbeat interval, then the client waits more than one heartbeat interval before it sends the aggregated event.</p>

## Miscellaneous: Notifications

You can configure notifications to appear on client computers when virus definitions are out-of-date or missing. You might want to alert users if you do not have automatic updates scheduled. In rare cases, users might see errors appear on their client computers during scans. For example, the client computer might encounter buffer overruns or decompression problems.

The options that appear on this tab depend on whether the client runs on a Windows or a Mac computer.

**Table 411: General notification options for Windows clients**

Option	Description
<b>When definitions are outdated</b>	<p>Displays a message on client computers when definitions are out-of-date.</p> <p><b>Days before a warning appears in Symantec Endpoint Protection</b> You can specify the number of days. The notification message appears when definitions are out of date by more than the specified number of days.</p> <p><b>Display a notification message on the client computer</b> You can customize the warning text.</p>
<b>When Symantec Endpoint Protection is running without virus definitions</b>	<p>Displays a message on client computers when the Symantec Endpoint Protection client is running without definitions</p> <p><b>Remediation attempts before a warning appears in Symantec Endpoint Protection</b> You can specify the number of attempts to update definitions. The notification message appears after the number of attempts to download fails. You can customize the warning message that appears on the client computer.</p> <p>For 14.3 RU3 and later clients, this setting is ignored. Instead, when definitions are out-of-date, Windows clients automatically check for the newer definitions at a regular interval. If the definitions are missing, the client logs an event once every 30 minutes.</p> <p><b>Display a notification message on the client computer</b> You can customize the warning text.</p>

Option	Description
<b>Display error messages with a URL to a solution</b>	<p>Enables or disables the error messages that appear on client computers and in the System log</p> <p>The error messages appear when users encounter the errors that are related to the system, licensing, installation, and Virus and Spyware Protection.</p> <p>In client control mode, error messages do not appear.</p> <p><b>You can choose to include one of the following types of URLs (uniform resource locations) in the error messages:</b></p> <ul style="list-style-type: none"> <li>• <b>Display the URL to a Symantec Technical Support Knowledge Base article</b> Displays a link to redirect users to an article about a specific error that users see. If an article does not exist, a prompt appears enabling users to send an email message to online technical support or phone support.</li> <li>• <b>Display a custom URL</b> Lets you enter a custom URL to direct users to a specific error that users see.</li> </ul>
<b>Customize Error Message</b>	Opens a dialog box in which you can edit the default error message that appears on client computers and in the System log.

**Table 412: General notification options for Mac clients**

Option	Description
<b>Display a warning when definitions are outdated</b>	<p>Displays a message on client computers when definitions are out-of-date</p> <p>You can specify the number of days. The notification message appears when definitions are out of date by more than the specified number of days.</p>

[The types of security policies](#)

## Customize Error Message

You can use this dialog to edit the error message that appears on client computers. This message also appears in the System log.

## Auto-Protect for Microsoft Outlook, Internet Email, or Lotus Notes: Actions

You can configure action and remediation options for Auto-Protect scans of Microsoft Outlook, Internet Email, or Lotus Notes.

### NOTE

A lock icon appears next to some options. Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

### NOTE

Auto-Protect for Internet Email and Lotus Notes are only available for client versions earlier than 14.2 RU1.

Table 413: Actions options

Detection type	Action options
<b>Malware</b>	<p>You can configure a first action to take and a second action to take if the first action fails. Click the <b>Override actions configured for Malware</b> check box to activate the actions.</p> <p>Click the icon to lock or unlock the first and second action settings on client computers.</p> <p><b>Actions for viruses include the following:</b></p> <ul style="list-style-type: none"> <li>• <b>Clean risk</b> (default first action): Tries to clean the infected file when a virus is found.</li> <li>• <b>Quarantine risk</b> (default second action): Tries to move the infected file to the Quarantine on the infected computer as soon as it is detected. After an infected file is moved to the Quarantine, a user on that client computer cannot run the file. The user must first specify an action for the file. For example, the user can specify that the client should clean the file and move the file back to its original location.</li> <li>• <b>Delete risk:</b> Tries to delete the file. Use this option only if you can replace the infected file with a virus-free backup copy. The file is permanently deleted and cannot be recovered from the recycle bin. If Auto-Protect cannot delete the file, detailed information about the action appears in the notification dialog box and the System log.</li> <li>• <b>Leave alone (log only):</b> Denies the access to the file, displays a notification, and logs the event. Use this option to take manual control of how Auto-Protect handles a virus. When you select this action, by default Symantec Endpoint Protection automatically deletes newly created or saved infected files. When you are notified of a virus, open the Risk log, right-click the name of the file, and select one of the following actions: Clean (viruses only), Delete Permanently, or Move To Quarantine.</li> </ul> <p><a href="#">Risk logs and quick reports</a></p>
<b>Security Risks</b>	<p>Click the <b>Override actions configured for Malware</b> check box to activate the actions. Click the icon to lock or unlock the first and second action settings on client computers.</p> <p><b>You can configure the following security risk actions:</b></p> <ul style="list-style-type: none"> <li>• Configure the same actions to take for all security risks.</li> <li>• Configure the same actions for a whole category of security risks.</li> <li>• Configure the individual security risk exceptions to the actions that you set for specific categories.</li> </ul> <p>You can configure a first action to take and a second action to take if the first action fails.</p> <p><b>Actions for security risks include the following:</b></p> <ul style="list-style-type: none"> <li>• <b>Quarantine risk</b> (default first action) Tries to move any infected files to the Quarantine on the infected computer as soon as the security risk is detected or completes its installation. Auto-Protect removes or repairs any side effects of the risk. Side effects might include additional registry keys, modified registry key values, additions to .ini or .bat files, or extra entries in hosts files. They might also include errors in a Layered Service Provider (LSP) system driver or the effects of a rootkit. You can restore the security risk items that are quarantined to their original state on the system. In some instances, you might need to restart the computer to complete the removal or repair.</li> <li>• <b>Delete risk</b> Tries to delete security risk files. Use this option only if you can replace the files with a security risk-free backup copy. You cannot recover permanently deleted files from the recycle bin. Use this action with caution. The deletion of security risks can cause applications to lose functionality. If the client cannot delete files, detailed information about the actions appears in the notification dialog box and the System log.</li> <li>• <b>Leave alone (log only)</b> (default second action) The risk is left alone and its detection is logged. Use this option to take manual control of how Auto-Protect handles a security risk. When you select this action, by default Symantec Endpoint Protection automatically deletes the newly created or saved files that are security risks You can use the Risk log in the console to specify the action for the logged risk. Users on client computers can use the logs to specify the action as well.</li> </ul> <p>You can also lock exceptions so that users cannot create their own security risk exceptions for all virus and spyware scans.</p> <p><b>Note:</b> In some instances, you might unknowingly install an application that includes a security risk such as adware or spyware. If Symantec determines that blocking the risk does not harm the computer, then by default, Auto-Protect blocks the risk. If the computer might enter an unstable state when Auto-Protect blocks the risk, Auto-Protect waits<sup>827</sup> until the application installation is complete. Then, Auto-Protect performs the configured action on the security risk.</p>

---

## Floppy Settings

You can set additional options for scanning floppies.

### NOTE

A lock icon appears next to some options. Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

**Table 414: Floppy settings options**

Option	Description
<b>Check floppies for boot virus when accessed</b>	Auto-Protect scans the floppy disk in the floppy drive for boot viruses when the drive is first accessed.
<b>When a boot virus is found</b>	When Auto-Protect finds a boot virus, select whether to clean a virus from the boot record or leave it alone. If you click <b>Leave alone (log only)</b> , an alert is sent when a virus is detected but no action is taken.

## Network Settings

You can configure additional options for network settings for Auto-Protect scans.

**Table 415: Network settings options**

Option	Description
<b>Trust files on remote computers running Auto-Protect</b>	Prevents Auto-Protect from performing duplicate scans while network scanning is enabled. If this option is enabled on two clients, each client checks to see that the other's Auto-Protect settings are as secure as its own. Each client then trusts the Auto-Protect scan on the other and does not rescan any files. For example, when client A accesses a file on a network drive on client B, client A's Auto-Protect checks client B's Auto-Protect settings. If client B's Auto-Protect is trustworthy, client A's Auto-Protect does not scan the file. If client B's Auto-Protect is not trustworthy, client A's Auto-Protect scans the file. Disable this setting if you want to allow duplicate scanning. Duplicate scanning can reduce network performance on the client computer. <b>Note:</b> This functionality applies only to read access. When client A requests write access from client B, client A's Auto-Protect scans the file regardless of this setting.
<b>Network cache</b>	Enables or disables a record of the files that Auto-Protect has already scanned from a network server This option prevents Auto-Protect from scanning the same file more than one time and may improve system performance. You can set the number of files (entries) that Auto-Protect scans and remembers. You can also set the timeout before the files are removed from the cache. After the timeout expires, Auto-Protect scans the network files again if the client requests them from the network server.

---

## Auto-Protect: Advanced

You can configure advanced options for Auto-Protect to use when it examines the file system.

### NOTE

A lock icon appears next to some options. Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

**Table 416: Advanced options for Auto-Protect**

Option	Description
Startup and Shutdown	<p><b>The following options are available:</b></p> <ul style="list-style-type: none"><li>• <b>Computer starts:</b> Loads Auto-Protect when the computer's operating system starts and unloads it when the computer shuts down. This option can help protect against some viruses. If Auto-Protect detects a virus during shutdown, it places the infected file in a temporary Quarantine folder. Auto-Protect then detects the virus on startup and creates an alert notification.</li></ul> <p><b>Note:</b> If you disable Auto-Protect on a computer that has this option enabled, Auto-Protect still functions after each computer restart for a brief time. When the main Symantec Endpoint Protection client service starts, it disables Auto-Protect.</p> <ul style="list-style-type: none"><li>• <b>Symantec Endpoint Protection starts:</b> Loads Auto-Protect when the client starts.</li><li>• <b>Check floppies when the computer shuts down:</b> Configures the client to scan floppies when the computer shuts down.</li></ul>
Auto-Protect Reloading and Enablement	<p><b>The following options are available:</b></p> <ul style="list-style-type: none"><li>• <b>Stop and reload Auto-Protect:</b> Stops and reloads Auto-Protect immediately.</li><li>• <b>Wait until the computer is restarted:</b> Stops and reloads Auto-Protect when the computer restarts.</li><li>• <b>When Auto-Protect is disabled:</b> You can re-enable Auto-Protect automatically after &lt;number&gt; number of minutes. Valid values range from 3 to 60.</li></ul> <p>This option is useful if users need to disable Auto-Protect on occasion.</p>
Additional Options	Sets the options for the file cache and Risk Tracer

## Internet Email Auto-Protect: Scan Details

For client versions earlier than 14.2 RU1, you can configure details for Auto-Protect scans of Internet email. For performance reasons, Auto-Protect for Internet email is not supported on server operating systems.

### NOTE

A lock icon appears next to some options. Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

Use exceptions to specify exclusions for files or folders.

[About the types of Auto-Protect](#)

[Creating exceptions for Virus and Spyware scans](#)

**Table 417: Scan Details options**

Option	Description
<b>Enable Internet Email Auto-Protect</b>	Enables or disables Auto-Protect for Internet email. Click the icon to lock or unlock this option on client computers.
<b>File types</b>	<p>Scans all file types or only files with selected extensions.</p> <p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Scan all files</b> Scans all files on the computer, regardless of type. Click the icon to lock or unlock this option on client computers.</li> <li>• <b>Scan only selected extensions</b> Scans only the files that have certain extensions. You can add more extensions for programs and documents if you have the files that use the extensions that are not already in the list. You can also reset this option to its default value.</li> <li>• <b>Select Extensions</b> Specifies that only certain file extensions should be included in the scan. You can add or remove file extensions to scan. Only the file extensions that you specify are scanned. Auto-Protect does not scan files with unlisted extensions.</li> </ul> <p><b>Note:</b> If you want to exclude files or directories from scans, create an exception. The exception applies to all scans that you run.</p>
<b>Compressed files</b>	<p>Specifies whether or not to scan files inside compressed files and how many levels to include</p> <p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Scan files inside compressed files</b> Scans the files that act as containers for a file or group of files. Click the icon to lock or unlock this option on client computers.</li> <li>• <b>Number of levels to expand if there are compressed files within compressed files</b> When a file archive (such as Files.zip) is scanned, the individual files of the archive are also scanned. If the archive itself contains compressed files, you can specify how many levels deep you want the compressed files to be scanned. The default setting is three levels deep in a compressed file.</li> </ul> <p><b>These types of compressed files may be included in virus scans:</b></p> <ul style="list-style-type: none"> <li>• .ARJ archive files, which are created by the ARJ* file compression software</li> <li>• .ZIP files, which are created by PKZip* and WinZip* file compression software</li> <li>• .LZH files compressed by Haruyasu Yoshizaki's Lharc* software</li> <li>• .EXE files created as self-extracting archives.</li> <li>• Compressed files without an extension.</li> </ul>

## Insert Warning

You can configure Auto-Protect to automatically insert a warning into the body of an infected email message. This warning can be important if the Symantec Endpoint Protection client cannot clean the virus from the message. The warning is

also important if an infected attachment is moved, left alone, deleted, or renamed. The Symantec Endpoint Protection client appends “Symantec Endpoint Protection found a security risk in an attachment from [EmailSender]” to the top of the infected email message.

Do not modify the fields in brackets, which contain variable information. You can customize the subject and body of the message.

**Table 418: Insert Warning options**

Option	Description
<b>Change the subject of the original message to</b>	Enables you to change the email subject. This option is enabled by default.
<b>Subject</b>	The subject of the email message The default is <b>Security risk found in message “[EmailSubject]”</b>
<b>Message body</b>	The text in the message body The default is <b>Symantec Endpoint Protection found a security risk in an attachment from [EmailSender].</b>
<b>Infection information</b>	The information about the infection that appears in the email message <b>The following information is listed for each infected file:</b> <ul style="list-style-type: none"> <li>• <b>Attachment</b> (name of the file attachment)</li> <li>• <b>Security risk detected</b> (Name of the security risk)</li> <li>• <b>Action taken</b> (such as cleaned, moved to the Quarantine, Deleted, or left alone)</li> <li>• <b>File status</b> (infected or not infected)</li> </ul>

**Table 419: Email message body fields**

Field	Description
<b>User</b>	The name of the user who was logged on when the virus or security risk occurred.
<b>DateFound</b>	The date on which the virus or security risk was found.
<b>EmailSender</b>	The email address that sent the email with the infected attachment.
<b>EmailRecipientList</b>	The list of addresses to which the email with the infected attachment was sent.

**Table 420: Infection information fields**

Field	Description
SecurityRiskName	The name of the virus or security risk that was found.
ActionTaken	The action that was taken in response to detecting the virus or security risk. This action can be either the first action or second action that was configured.
Status	The state of the file: Infected, Not Infected, or Deleted. This message variable is not used by default. To display this information, manually add this variable to the message.
Filename	The name of the file that the virus or security risk infected.
PathAndFilename	The complete path and name of the file that the virus or security risk infected.
Computer	The name of the computer on which the virus or security risk was found.
User	The name of the user who was logged on when the virus or security risk occurred.

Field	Description
DateFound	The date on which the virus or security risk was found.
OriginalAttachmentName	The name of the attachment that contains the virus or security risk.
StorageName	The affected area of the application such as Auto-Protect for files and processes or Microsoft Outlook Auto-Protect.

## Email Server

To notify the sender of an infected message, you must specify the email server to use to send the message.

**Table 421: Email server options**

Option	Definition
<b>Mail server</b>	Name of the mail server that sends the notification
<b>Mail port</b>	Mail port that is to be used to send the message; the default is <b>25</b>
<b>User name</b>	User name required to access the mail server and send messages
<b>Password</b>	Password that the mail server requires
<b>Reverse-path</b>	Reverse-path information if your mail server requires it The reverse path is usually not necessary. If the mail server requires it, you can type the DNS name of the computer that generates the message.

## Message

You can customize the email message that is sent to the sender of an infected email message or to the recipient list.

**Table 422: Message options**

Option	Definition
<b>Subject</b>	The text for the subject of the email message The default is <b>Security risk found in message “[EmailSubject]”</b>
<b>Message body</b>	The text for the body of the email message The default is <b>Symantec Endpoint Protection found a security risk in an attachment you ([EmailSender]) sent to [EmailRecipientList]. To ensure the recipients are able to use the files you send, perform a virus scan on your computer, clean any infected files, then resend this attachment.</b>
<b>Infection information</b>	The infection information that is included in the email message <b>You can add what infection information to include in the email:</b> <ul style="list-style-type: none"> <li>• <b>Attachment</b> (name of the attachment)</li> <li>• <b>Security risk detected</b> (name of the security risk)</li> <li>• <b>Action taken</b> (such as cleaned or left alone)</li> <li>• <b>File status</b> (infected or not infected)</li> </ul>



---

**Table 423: Email message body fields**

Field	Description
EmailSender	The email address that sent the email with the infected attachment.
EmailRecipientList	The list of addresses to which the email with the infected attachment was sent.

**Table 424: Infection information fields**

Field	Description
SecurityRiskName	The name of the virus or security risk that was found.
ActionTaken	The action that was taken in response to detecting the virus or security risk. This action can be either the first action or second action that was configured.
Status	The state of the file: Infected, Not Infected, or Deleted. This message variable is not used by default. To display this information, manually add this variable to the message.
Filename	The name of the file that the virus or security risk infected.
PathAndFilename	The complete path and name of the file that the virus or security risk infected.
Computer	The name of the computer on which the virus or security risk was found.
User	The name of the user who was logged on when the virus or security risk occurred.
DateFound	The date on which the virus or security risk was found.
OriginalAttachmentName	The name of the attachment that contains the virus or security risk.
StorageName	The affected area of the application such as Auto-Protect for files and processes, or Microsoft Outlook Auto-Protect.

## Send Email to Others: Others

You can automatically notify others about a virus or security risk infection.

Type the email addresses of the individuals who should be automatically notified about a virus or security risk. The Symantec Endpoint Protection client sends an email message that contains information about the security risk to the addressees in the list. You can add or remove email addresses.

## Internet Email Auto-Protect: Advanced

For client versions earlier than 14.2 RU1, you can configure connection settings for Auto-Protect scans of Internet email.

### NOTE

A lock icon appears next to some options. Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

**Table 425: Advanced options for Auto-Protect scans of Internet email**

Option	Description
Connection Settings	<p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Incoming mail server (POP3)</b> Auto-Protect scanning for Internet email uses the standard POP3 email ports by default. If you configure your network to use a different port, you must change the port setting here to match the port that you selected. Click the icon to lock or unlock this option on client computers.</li> <li>• <b>Outgoing mail server (SMTP)</b> Auto-Protect scanning for Internet email uses the standard SMTP email ports by default. If you configure your network to use a different port, you must change the port setting here to match the port that you selected.</li> <li>• <b>Use Defaults</b> Returns the Incoming mail server (POP3) and Outgoing mail server (SMTP) port settings to their defaults.</li> </ul>
Encrypted Connections	<p>Click the icon to lock or unlock these options on client computers.</p> <p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Allow encrypted POP3 connections</b> Use this option to enable or disable POP3 messages that use encrypted connections. Auto-Protect does not scan any email that uses POP3 over the Secure Sockets Layer (SSL). Auto-Protect continues to protect computers from viruses and security risks in attachments.</li> <li>• <b>Allow encrypted SMTP connections</b> Use this option to enable or disable the SMTP messages that use encrypted connections. Auto-Protect does not scan any email that uses SMTP over the Secure Sockets Layer (SSL). Auto-Protect continues to protect computers from viruses and security risks in attachments.</li> </ul> <p><b>Note:</b> The client cannot scan any messages that are sent or received over encrypted connections. If you disable the encrypted options, Auto-Protect blocks the messages. The change does not take effect until the user logs off Windows and logs on again.</p>
Mass Mailing Worm Heuristics	<p>Click the icon to lock or unlock these options on client computers.</p> <p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Outbound worm heuristics</b> Use this option to scan outgoing messages for suspicious behavior.</li> <li>• <b>First action</b> Select an action to take when the scan detects suspicious behavior. You can choose to quarantine the threat, delete the threat, or to log the detection but take no action on the threat.</li> <li>• <b>If first action fails</b> Select an action to take when the scan cannot perform the first action on the detected threat. You can choose to delete the threat or to log the detection but take no action on the threat.</li> </ul> <p><b>Note:</b> If you set the First action to Leave alone (log only), then this option is not available.</p>

---

## Microsoft Outlook Auto-Protect: Scan Details

You can configure details for Auto-Protect scans of Microsoft Exchange email clients.

**NOTE**

A lock icon appears next to some options. Click the icon to lock or unlock the option. When you lock an option, you prevent changes to the option on client computers.

[About the types of Auto-Protect](#)

[Creating exceptions for Virus and Spyware scans](#)

**Table 426: Scan details options**

Option	Description
Enable Microsoft Outlook Auto-Protect	Enables or disables Auto-Protect for Microsoft Exchange email clients (Outlook)
File types	<p>Scans all file types or only files with selected extensions.</p> <p><b>The following options are available:</b></p> <ul style="list-style-type: none"><li>• <b>Scan all files</b> Scans all files on the computer, regardless of type.</li><li>• <b>Scan only selected extensions</b> Scans only the files that have certain extensions. You can add more extensions for programs and documents, if you have the files that use the extensions that are not already in the list. You can also reset this option to its default value.</li></ul> <p><b>Select Extensions</b> Specifies that only certain file extensions should be included in the scan.</p> <p>You can add or remove file extensions to scan. Only the file extensions that you specify are scanned. Auto-Protect does not scan files with unlisted extensions.</p> <p><b>Note:</b> If you want to exclude files or folders from scans, create an exception.</p>

Option	Description
Compressed files	<p>Specifies whether or not to scan files inside compressed files and how many levels to include</p> <p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Scan files inside compressed files</b> Scans the files that act as containers for a file or group of files.</li> <li>• <b>Number of levels to expand if there are compressed files within compressed files.</b> When a file archive (such as Files.zip) is scanned, the individual files of the archive are also scanned. If the archive itself contains compressed files, you can specify how many levels deep you want the compressed files to be scanned. The default setting is three levels deep in a compressed file.</li> </ul> <p><b>These types of compressed files may be included in virus scans:</b></p> <ul style="list-style-type: none"> <li>• .ARJ archive files, which are created by the ARJ* file compression software.</li> <li>• .ZIP files, which are created by PKZip* and WinZip* file compression software.</li> <li>• .LZH files compressed by Haruyasu Yoshizaki's Lharc* software.</li> <li>• .EXE files created as self-extracting archives.</li> <li>• Compressed files without an extension.</li> </ul>

## Lotus Notes Auto-Protect: Scan Details

For client versions earlier than 14.2 RU1, you can configure details for Auto-Protect scans of Lotus Notes email.

### NOTE

A lock icon appears next to some options. Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

**Table 427: Scan Details options**

Option	Description
<b>Enable Lotus Notes Auto-Protect</b>	Enables or disables Auto-Protect for Lotus Notes
<b>File types</b>	<p>Scans all file types or only files with selected extensions.</p> <p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Scan all files</b> Scans all files on the computer, regardless of type.</li> <li>• <b>Scan only selected extensions</b> Scans only the files that have certain extensions. You can add more extensions for programs and documents, if you have the files that use the extensions that are not already in the list. You can also reset this option to its default value.</li> </ul> <p><b>Note:</b> If you want to exclude files or folders from scans, create an exception.</p>

Option	Description
<b>Select Extensions</b>	<p>Specifies that only certain file extensions should be included in the scan</p> <p>You can add or remove file extensions to scan. Only the file extensions that you specify are scanned. Auto-Protect does not scan files with unlisted extensions.</p> <p><b>Note:</b> If you want to exclude files or folders from scans, create an exception.</p>
Compressed files	<p>Specifies whether or not to scan files inside compressed files and how many levels to include</p> <p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Scan files inside compressed files</b> Scans the files that act as containers for a file or group of files.</li> <li>• <b>Number of levels to expand if there are compressed files within compressed files</b> When a file archive (such as Files.zip) is scanned, the individual files of the archive are also scanned. If the archive itself contains compressed files, you can specify how many levels deep you want the compressed files to be scanned. The default setting is three levels deep in a compressed file.</li> </ul> <p><b>These types of compressed files may be included in virus scans:</b></p> <ul style="list-style-type: none"> <li>• .ARJ archive files created by the ARJ* file compression software</li> <li>• .ZIP files created by PKZip* and WinZip* file compression software</li> <li>• .LZH files compressed by Haruyasu Yoshizaki's Lharc* software</li> <li>• .EXE files created as self-extracting archives.</li> <li>• Compressed files without an extension.</li> </ul>

## Outdated Virus Definitions Warning

You can modify the default message that appears on client computers when virus definitions are out-of-date.

## Absent Virus Definitions Warning

You can modify the default message that appears when the client computer does not have any virus definitions.

## Administrator-defined Scans: Scans

You can use the **Scans** tab to add or edit a scheduled scan to a policy, or to specify settings for on-demand scans. On-demand scans are the manual scans that run on a client at the administrator's request.

Administrators define scheduled scans to run on client computers at configurable intervals. Administrators can predefine a specific set of scan settings for running on-demand scans on clients from the console.

Under **Administrator On-demand Scan**, click **Edit** to specify the type of scan that occurs when an administrator activates a scan from the console.

[About the types of scans and real-time protection](#)

[Setting up scheduled scans that run on Windows computers](#)

---

## Add Scheduled Scan

Use this dialog box to create a new scheduled scan or a scan that is based on a scan template.

**Table 428: New scan options**

Option	Description
Create a new scheduled scan	Creates a new scheduled scan with default settings When you select this option and click OK, the New Scan dialog box appears. You can use that dialog box to configure the scan schedule, scan actions, notification settings, and other details.
Create a scheduled scan from a Scheduled Scan Template	Lets you select a template from the list to base this scan on

## Scan Details

You can use this tab to set options for this scan on Windows computers. You can specify the name, the description, and the scan type, and you can choose advanced scanning options.

**Table 429: Scan Details options**

Option	Description
<b>Operating System</b>	Not configurable for scheduled scans. <b>Note:</b> If you are adding a scan template, you can select either the Windows or Mac operating system. If you change the operating system, click Help again to get help on the relevant options.
<b>Scan name</b>	Specifies the name you want to use for the scan. For Administrator on-demand scans, the scan name is <b>Administrator On-demand Scan</b> , which cannot be changed.
<b>Description</b>	Provides a description of the scan for future reference. For Administrator on-demand scans, the description is a default on-demand scan description, which cannot be changed.
<b>Scan type</b>	Specifies the type of scan to run. For Administrator on-demand scans, there is no scan type. <b>For all other scans, you can select from the following options:</b> <ul style="list-style-type: none"><li>• <b>Active Scan</b> Scans the system memory and all the common virus and security risk locations on the computer very quickly. The scan includes all processes that run in memory, important registry files, and files like config.sys and windows.ini. It also includes some critical operating system folders.</li><li>• <b>Full Scan</b> Scans the entire computer for viruses and security risks, including the boot sector and system memory. This scan includes all folders and files. You cannot change the settings for this scan.</li><li>• <b>Custom Scan</b> Scans the files and folders that you select for viruses and security risks. You can specify which folders and files to scan for custom scans.</li></ul>

Option	Description
<b>Scanning</b>	<p><b>Edit Folders</b> is enabled when the <b>Custom Scan</b> is selected for <b>Scan type</b> and for Administrator on-demand scans.</p> <p>Specifies which folders and files to scan</p> <p>This setting is useful to save scanning time and computer resources.</p> <p><b>Note:</b> This option is not available for active scans and full scans.</p>
<b>File types</b>	<p>Specifies the types of files be scanned.</p> <p>You can scan all files or limit the scan to files with specific extensions.</p>
<b>Enhance the scan by checking</b>	<p>Specifies the additional locations to scan on the client computer.</p> <p><b>The following options are available for custom scans:</b></p> <ul style="list-style-type: none"> <li>• <b>Memory</b> Scans the memory in addition to all files or the types of files or directories that you selected</li> <li>• <b>Common infection locations</b> Scans the common infection locations in addition to all files or the types of files or directories that you selected</li> <li>• <b>Well-known virus and security risk locations</b> Scans the well-known virus and security risk locations in addition to all files or the types of files or directories that you selected.</li> </ul>
<b>Advanced Scanning Options</b>	<p>You can configure advanced scan options for compressed files, storage migration, and performance.</p>
<b>Enable Insight Lookup</b>	<p>Insight Lookup uses the latest virus definitions in the cloud as well as reputation data to evaluate files. Reputation data is the information that Symantec collects about the potential maliciousness of a file.</p> <p>When you enable this option, Insight Lookup detects the files that might not typically be detected as risks.</p> <p>For Symantec Endpoint Protection client versions earlier than 14 that are managed by Symantec Endpoint Protection Manager 14, Insight Lookup uses sensitivity levels and actions that are configured for Download Insight detections. For 14 clients, Insight Lookup uses internal settings to optimize sensitivity levels and actions during the scan.</p>

## Advanced Scanning Options: Compressed Files

Use this tab to set the options for scanning compressed files.

### NOTE

A lock icon appears next to some options. Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

**Table 430: Advanced scanning options for compressed files**

Option	Description
<b>Scan files inside compressed files</b>	<p>Enables the scanning of containers, such as Files.zip, and the contents of the containers, which are the individual compressed files.</p> <p>Symantec Endpoint Protection scans compressed files during on-demand, email, and scheduled scans. When this option is enabled and you use the <b>Extensions</b> dialog to include only specified file extensions, Symantec Endpoint Protection continues to scan container files and their contents even if you do not specify the container file extensions. You can disable the <b>Scan files inside compressed files</b> option or create exceptions for specific container file extensions so that scans do not scan them.</p> <p>Because of the significant processing overhead, Auto-Protect does not scan the files that are within compressed files on Windows computers. However, the files are scanned when they are extracted from compressed files.</p> <p><b>Note:</b> You cannot stop a scan that is in progress on a compressed file. If you choose to stop the scan, the Symantec Endpoint Protection client stops the scan only after it has finished scanning the compressed file.</p>
<b>Number of levels to expand if there are compressed files within compressed files</b>	<p>Specifies the number of levels of nesting scans should support.</p> <p>The client supports a maximum depth of ten levels of nested compressed files for Windows computers. The default setting is three levels.</p>

## Advanced Scanning Options: Storage Migration

Use this tab to fine-tune scans of the files that Hierarchical Storage Management (HSM) and offline backup systems maintain. An HSM system migrates files to secondary storage such as DVD-ROM, tape jukebox, or SAN storage. The system might leave parts of the original file on the disk, however.

**Performance and disk space issues can arise if the following situations are true:**

- The Symantec Endpoint Protection client scans the stubs.
- The HSM system places the files back on the original disk.

### NOTE

For all of these options, consult your HSM or backup vendor to select the appropriate settings.

**Table 431: Storage migration options**

Option	Description
Skip offline files	<p>Specifies that if the offline bit is set, the Symantec Endpoint Protection client skips the file</p> <p>A small clock over a file's icon in Windows Explorer indicates that the offline bit is set. Any application can set the offline bit even if the file is not offline.</p>
Skip offline and sparse files	<p>Specifies that offline and sparse files are skipped</p> <p>Some applications set the file sparse bit to indicate that part of the file is not present on the disk. Some HSM products set this bit and others don't. With a sparse file, a stub of the file remains on the disk, and the majority of the file is moved to offline storage. This setting is the default.</p>
Skip offline and sparse files with a reparse point	<p>Specifies that offline and sparse files with a reparse point are skipped</p> <p>Some vendors use reparse points. Applications that use reparse points also use an appropriate device driver to manage reparse points in the files. With a reparse point, a portion of the file remains on disk, and the remainder is transparently accessed through the device driver.</p>



Option	Description
Scan resident portions of offline and sparse files	Specifies that if the file is sparse, the Symantec Endpoint Protection client scans only the resident portion. The Symantec Endpoint Protection client identifies resident portions of a file. The nonresident portion remains in secondary storage. Some vendors support this capability.
Scan all files, forcing demigration (fills drive)	The Symantec Endpoint Protection client scans the entire file, which forces demigration from secondary storage if necessary. Because the size of the secondary storage is usually greater than the size of the local volume, this setting might fill the local volume. When the local volume is full, further files that are opened for scanning might fail.
Scan all files without forcing demigration (slow)	Specifies that all files are scanned, without forcing demigration. The Symantec Endpoint Protection client copies a file from secondary storage to the local hard drive as a temp file for scanning. The HSM application leaves the original file on the secondary storage. This method is slow and not all HSM vendors support it. Because a file is copied from secondary storage to a disk for scanning, resource demand is high. Processor and network performance might further degrade as the Symantec Endpoint Protection client detects infected content when a repair or deletion is returned to secondary storage.
Scan all files recently touched without forcing demigration	Specifies that all files that have been touched recently are scanned, without forcing demigration. This option lets you specify that only the files that have been migrated recently and might still reside on faster secondary storage are scanned. This method can reduce some of the resource demand issues with the Scan all files without forcing demigration option. You can scan the files that reside on faster disks, and skip demigration and scans if the files reside on slow disks. For example, files might be migrated to a remote disk after 30 days of no access. After 60 days of no access, the file is migrated to DVD-ROM or remote SAN storage. This method might still be slow because file access without forced demigration can be a slow operation. If you select this option, you must select the type of access and the number of days to define "recently touched."
Open files using backup semantics	Specifies that files be opened using backup semantics. In some cases, using this option may allow the Symantec Endpoint Protection client to scan files without demigration. It may also allow the client to scan the stub, but not the rest of the demigrated file.
Type of access within the number of days selected	If you select Scan all files recently touched without forcing demigration, you must set this option. This option specifies the type of access (Accessed, Modified, or Created) and the number of days to define as "recent."

## Advanced Scanning Options: Tuning

Use this tab to move the slider to set the scan performance priority.

**Table 432: Optimizing performance options**

Option	Description
<b>Best Scan Performance</b>	Optimizes the performance of the scans that run on the computer. Scans take less time to complete, but other applications may run more slowly during scans. For computers with four or more CPUs, use this option for the best overall performance.
<b>Balanced Performance</b>	Balances the performance of a scan against the performance of other applications. Balances scan performance and the performance of other applications that run during scans.
<b>Best Application Performance</b>	Optimizes the performance of other applications that are running on the computer. Scans take longer to complete, but other applications on the computer may perform better during a scan. When this option is set, scans can start but they only run when the client computer is idle. If you configure an Active Scan to run when new definitions arrive, the scan is delayed for up to 15 minutes if the user is using the client computer.

---

## Scheduled Scan: Schedule

You can set scan times, randomize scan start times, and specify the retry interval if scans are missed.

You can specify a time when to run the scan daily, weekly, or monthly. The exact time that the scan actually runs depends on the last run time of the scan, whether or not the scan time is randomized, and the settings for missed scans.

### NOTE

You can specify the scan duration and the retry interval for Windows clients only. Limitations on scans and randomized scans are not available for Mac clients. Mac clients do not try to scan again if a scheduled scan is missed.

Table 433: Schedule options

Option	Description
Scanning Schedule	<p>Specifies the frequency of the scan.</p> <ul style="list-style-type: none"> <li>• <b>Daily</b> lets you select the time the scan runs each day. The actual time that the scan runs is based on the last run time and the scan duration and missed scheduled scan settings.</li> <li>• <b>Weekly</b> lets you select the time and day the scan runs each week. The actual time that the scan runs is based on the last run time and the scan duration and missed scheduled scan settings.</li> <li>• <b>Monthly</b> lets you select the time and day the scan runs each month. The actual time that the scan runs is based on the last run time and the scan duration and missed scheduled scan settings.</li> </ul> <p>Symantec Endpoint Protection might not use the configured time if the last run of the scan occurred at a different time because of the scan duration or missed scheduled scan settings. For example, you might configure a weekly scan to run every Sunday at midnight and a retry interval of one day. If the computer misses the scan and starts up on Monday at 6am, the scan runs at 6am. The next scan is performed one week from Monday at 6am rather than the next Sunday at midnight.</p> <p>If the computer did not start until Tuesday at 6am, which exceeds the retry interval by two days, the computer does not retry the scan. The computer waits until the next Sunday at midnight to try to run the scan.</p> <p>In either case, if you randomize the scan start time you might change the last run time of the scan.</p>
Scan Duration	<p>Supported on clients that run Windows.</p> <p>Specifies how long a scan should run. You can specify any of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Scan until finished</b> This setting is recommended in most cases to optimize scan performance.</li> <li>• <b>Scan for up to n hours</b> This setting lets you control scan times in environments where resources may be limited. If a scan does not finish within the time period that is specified, the scan resumes at the next scheduled time. For randomized scans, the scan resumes at a randomized time during the specified interval. For example, if you configure the scan to run at 8:00pm and set the duration for up to 4 hours, a non-randomized scan starts or resumes at 8:00pm. For randomized scans, the scan starts or resumes at a randomly selected minute between 8:00pm and midnight.</li> </ul> <p>If you choose to limit the scan time, you can also specify <b>Randomize scan start time within this period</b>. Use this setting to scan virtual machines. Randomizing scans minimizes the chance of multiple scans starting at the same time and requiring high resource use on the host computer.</p> <p>If you set the frequency to <b>Daily</b>, the maximum scan duration is 23 hours. If you set the frequency to <b>Weekly</b>, the maximum scan duration is 167 hours. If you set the frequency to <b>Monthly</b>, the maximum scan duration is 671 hours.</p>

Option	Description
<b>Missed Scheduled Scans</b>	<p>Supported on clients that run Windows</p> <p>You can specify a time interval to retry a scan that did not start as scheduled. For example, a scan might be missed because the computer was off or hibernation or sleep mode. When the computer starts or wakes, Symantec Endpoint Protection retries the scan until the scan starts or the retry interval expires. If the retry interval already expired, then Symantec Endpoint Protection skips the scan and waits for the next scheduled scan.</p> <p><b>Retry the scan within</b> specifies the number of hours or days during which Symantec Endpoint Protection can retry a missed scan.</p> <p>If you set the frequency to <b>Daily</b>, the maximum retry interval is 72 hours. If you set the frequency to <b>Weekly</b>, the maximum retry interval is seven days. If you set the frequency to <b>Monthly</b>, the maximum retry interval is 11 days. The defaults are the same as the maximums, except for weekly scans, which have a default of three days.</p>

## Administrator-defined Scans: Advanced

Use this tab to set options for scheduled scans and startup and triggered scans, and for users on the computers that run these scans.

**Table 434: Scheduled scans advanced options**

Option	Description
<b>Scheduled Scans</b>	Specified options for scheduled scans.
<b>Delay scheduled scans when running on batteries</b>	<p>Specifies that scheduled scans be delayed when a computer is running on batteries. This option is enabled by default. You can disable this option to allow scheduled scans to run as scheduled, even when a computer is running on batteries.</p>
<b>Allow user-defined scheduled scans to run when the scan author is not logged on</b>	<p>Specifies that user-defined scheduled scans run as scheduled when the scan author is not logged on.</p> <p>By default, user-defined scheduled scans always run at the scheduled time. This option can be particularly useful in the case of unmanaged client computers that do not use administrator-defined scheduled scans.</p> <p>You can disable this option to prevent user-defined scheduled scans from running when the user who created the scan is not logged on. You may want to disable this option for multiuser computers.</p> <p><b>Note:</b> If this option is enabled and the user is logged off when the scan begins, the scan progress dialog box does not display. You can check scan status in this instance by looking in the System log.</p> <p><b>On multiuser workstations, when this option is enabled, scan progress is displayed as follows:</b></p> <ul style="list-style-type: none"> <li>• If no users are logged on, the scan progress dialog box does not appear, even if a user logs on during a scan.</li> <li>• For the first user to log on, the scan progress dialog box does not appear during a scheduled scan that another user defined.</li> <li>• For the first user to log on, the scan progress dialog box appears during a scheduled scan that this user defined. The scan progress dialog box does not appear if the user has not configured the scan to allow it.</li> <li>• If an administrator-defined scheduled scan runs when no user is logged on, the scan progress dialog box does not appear. When a user logs on, the scan progress dialog box appears.</li> </ul> <p>Users who are not logged on when their scan runs must look at the Scan Log to see the scan results.</p>

Option	Description
<b>Display notifications about detections when the user logs on</b>	Displays notifications when a user logs on and scans have been running in the background. The option is enabled by default. The administrator can disable this option to have a completely silent application, with no notifications displayed to the user.

**Table 435: Startup and triggered scan advanced options**

Option	Description
<b>Allow startup scans to run when users log on</b>	Allows startup scans to run when a user logs on. This option applies to all startup scans. If you disable this option, startup scans do not run when users log on.
<b>Allow users to modify startup scans</b>	Determines whether users can modify startup scans. This option is enabled by default. You can change this option only when the <b>Run startup scans when users log on</b> parameter is enabled.
<b>Run an Active Scan when new definitions arrive</b>	Starts an Active Scan when new definitions arrive to check for any risks that the new definitions can detect By default, an Active Scan is run when new definitions arrive. If you disable this option, you weaken the protection available to your client computers. You should only disable this option if you have special configuration or exclusion needs that conflict with this automatically triggered scan. If you set the tuning option for an Active Scan to <b>Best Application Performance</b> , the active scan might wait to start up to 15 minutes if the computer is not idle.

**Table 436: Scan progress options**

Option	Description
<b>Select scan progress options</b>	Specifies what users see on their computers when a scan is running. <b>Select one of the following:</b> <ul style="list-style-type: none"> <li>• <b>Do not show scan progress</b></li> <li>• <b>Show scan progress</b></li> <li>• <b>Show scan progress if risk detected</b></li> <li>• <b>Show scan progress if medium or higher risk impact detected</b></li> </ul> <b>When you allow users to view scan progress, the following options appear in the main pages of the client UI:</b> <ul style="list-style-type: none"> <li>• When a scan runs, the message link <b>scan in progress</b> appears. The user can click the link to display the scan progress.</li> <li>• A link to reschedule the next scheduled scan also appears.</li> </ul>
<b>Close the scan progress window when done</b>	Specifies that the scan progress window closes automatically when the scan is finished. This option is available when you select either <b>Show scan progress</b> or <b>Show scan progress if risk detected</b> . This option is enabled by default.
<b>Allow the user to stop the scan</b>	Allows users to stop the scans that start on their computers. This option is available when you select either <b>Show scan progress</b> or <b>Show scan progress if risk detected</b> . This option is disabled by default.
<b>Allow the user to pause or snooze a scan</b>	Allows the users to pause or snooze the scans that start on their computers. This option is available when you select either <b>Show scan progress</b> or <b>Show scan progress if risk detected</b> . This option is enabled by default. When this option is enabled, click <b>Pause Options</b> to specify pause and snooze options. The <b>Snooze</b> option applies on user-defined scheduled scans only.

---

## Scan Pause Options

You can use this dialog box to set the options that relate to scan interruptions and delays. When a user pauses a scan, the **Scan Results** dialog box remains open. If the computer is turned off, the paused scan does not continue. When a user snoozes a scan, the **Scan Results** dialog box closes, and reappears when the snooze period ends and the scan resumes.

**Table 437: Scan pause options**

Option	Description
<b>Limit the time the scan may be paused</b>	Limits the amount of time a user can pause an administrator-defined scheduled scan This option is disabled by default. When the option is enabled, specify the number of minutes to pause the scan.
<b>Minutes to pause the scan</b>	Specifies the number of minutes that you want to allow users to pause this scan This option is enabled when the <b>Limit the time the scan may be paused</b> option is enabled. The default value is 60 minutes, and the range is 3 minutes to 180 minutes.
<b>Maximum number of snooze opportunities</b>	Specifies the number of times to allow a user to delay this scan This option is set to 3 by default. The allowed range is 1 time to 8 times.
<b>Allow users to snooze the scan for 3 hours</b>	Allows users to pause a scan for three hours. The option to delay the scan for one hour is enabled by default. The <b>Snooze</b> option applies on user-defined scheduled scans only.

## Quarantine: Cleanup

You can use this option to enable the automatic deletion of repaired, backup, and quarantined files from the computer. You can delete the files based on file age, folder size, or both. If you set both types of limits, then all files older than the time you have set are deleted first. If the size of the folder still exceeds the limit, then the oldest files are deleted until the folder size falls below the limit. By default, these options are enabled.

**Table 438: Cleanup options**

Option	Description
<b>Enable automatic deleting of &lt;repaired files   backup files   quarantined files that could not be repaired&gt;</b>	Enables the automatic deletion of any files that cannot be repaired.
<b>Delete after</b>	Specifies the number of days to keep the files. The maximum is 30 days.
<b>Delete oldest files to limit folder size at N (MB)</b>	Specifies the maximum size the folder can reach. The default is 50 MB.

## Common Settings for Mac client scans

You use the Common Settings tab to specify options for scheduled scans. These options do not apply to on-demand scans.

**Table 439: Common settings for Mac client scans**

Option	Description
<b>Scan compressed files</b>	Use this option to include compressed files in administrator-defined scans. The scan includes the compressed file and the files inside the compressed file.
<b>Allow scan snooze</b>	Use this option to let the user of the client computer delay the scan before it begins. The user cannot snooze a scan in progress.  <b>Note:</b> If you enable this option, be aware that you cannot set the maximum number of times the user delays the scan on the Mac client.
<b>Allow scan cancel</b>	Use this option to let the user of the client computer cancel the scan.
<b>Actions</b>	Specify the following actions that the scan takes when it detects a risk: <ul style="list-style-type: none"> <li>• <b>Automatically repair infected files</b> Symantec Endpoint Protection automatically tries to repair the infected file when a risk is found. If you do not choose this option, any repair must be performed manually.</li> <li>• <b>Quarantine the files that cannot be repaired</b> Symantec Endpoint Protection automatically moves any file that cannot be repaired to the Quarantine.</li> </ul> <p><b>Warning!</b> If you do not choose <b>Automatically repair infected files</b>, any infected files are not moved to the Quarantine, even if you choose <b>Quarantine the files that cannot be repaired</b>.</p> <p><b>Warning!</b> The software asks whether you want to repair an infected file. If you do not repair the file, it is left on the computer. If you choose <b>Automatically repair infected files</b>, and if you do not choose <b>Quarantine the files that cannot be repaired</b>, any infected files are deleted.</p>
<b>Alerts</b>	Choose from the following options on how the scan handles alerts: <ul style="list-style-type: none"> <li>• <b>Show only when infected files are found</b> Shows an alert only when a scan finds an infected file.</li> <li>• <b>Show when any scheduled scan is completed</b> Shows an alert when a scheduled scan finishes.</li> </ul>

## Mac Auto-Protect and SONAR: Scan Details

You can specify Auto-Protect actions, the files that Auto-Protect scans, and how Auto-Protect behaves when external disks or devices are connected to a Mac client.

### NOTE

A lock icon appears next to **Lock Auto-Protect settings**. Click the icon to lock or unlock Auto-Protect settings on Mac client computers. When you lock Auto-Protect settings, you prevent user changes to the settings.

### WARNING

If you do not choose **Automatically repair infected files**, any infected files are not moved to the Quarantine, even if you choose **Quarantine the files that cannot be repaired**.

The software asks whether you want to repair an infected file. If you do not repair the file, it is left on the computer. If you choose **Automatically repair infected files**, and if you do not choose **Quarantine the files that cannot be repaired**, any infected files are deleted.

**Table 440: Auto-Protect scan details for Mac clients**

Option	Description
<b>Lock Auto-Protect settings</b>	Click the icon to lock or unlock Auto-Protect settings on Mac client computers.
<b>Enable Auto-Protect</b>	You can enable or disable Auto-Protect scans for Mac clients.
<b>Automatically repair infected files</b>	You can choose to have Auto-Protect automatically repair any infected files that it finds.
<b>Quarantine files that cannot be repaired</b>	You can choose whether to send any files that cannot be repaired to the Quarantine.
<b>Scan compressed files</b>	You can choose whether to include compressed files in an Auto-Protect scan. The scan includes the compressed file and the files inside the compressed file.
<b>Scan Mounted Disk Details</b>	<p>You can choose to have Auto-Protect scan a mounted disk or device when a file on the disk or device is opened or copied. The following options are available:</p> <p>You can choose to scan only data disks, all other disks and devices, or both. The <b>Data disks</b> option includes software CDs or DVDs. The <b>All other disks or devices</b> option includes mounted disk images as well as audio or video CDs or DVDs.</p> <p>The legacy client settings do not apply to 12.1.4 clients and later.</p>
<b>Suspicious Behavior Detection</b>	<p>You can enable or disable detection of trusted applications that exhibit suspicious behavior.</p> <p>This option is available as of version 14.3 RU1.</p>

## Legacy client settings: Scan Mounted Disk Details (Mac only)

You can specify how to scan disks or devices when they are mounted on legacy clients.

### NOTE

These options do not apply to 12.1.4 clients and later.

**Table 441: Scan mounted disk options**

Option	Description
<b>Scan disks when they are mounted</b>	Enables Auto-Protect scans of mounted disks or devices.
<b>Show progress during scans of mounted disks</b>	Lets you view scan progress when Auto-Protect scans a mounted disk or device.
<b>Scan the following disks or devices:</b>	<p>Lets you specify the types of mounted disks or devices that Auto-Protect scans. You can run a scan on <b>All</b> mounted disks or devices, or on only <b>Music or video disks</b>, <b>iPod players</b>, <b>Data disks</b>, or <b>All other disks</b>.</p> <p><b>Note:</b> The <b>All other disks</b> option includes mounted disk images.</p>

## On-demand scan details for Mac clients

You can specify drives and folders to scan for on-demand scans. You can also specify the actions that a scan takes when it detects a risk.

### NOTE

You cannot specify the scan type for Mac clients. Different scan types are available only for Windows clients. Mac clients always run custom scans. If you run an active scan command on a group that includes Mac clients and Windows clients, the Windows clients run the active scan. The Mac clients, however, run a custom scan.



**Table 442: On-demand scan details**

Option	Description
Scan drives and folders	You can specify whether to scan hard drives or removable drives, or both. You can also select which folders to scan and whether to scan compressed files.
Actions	<p>Specify the actions that the scan takes when it detects a risk.</p> <p>You can choose either or both of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Automatically repair infected files</b> Symantec Endpoint Protection automatically tries to repair the infected file when a risk is found. If you do not choose this option, any repair must be performed manually.</li> <li>• <b>Quarantine files that cannot be repaired</b> Symantec Endpoint Protection automatically moves any file that cannot be repaired to the Quarantine.</li> </ul> <p><b>Warning!</b> If you do not choose <b>Automatically repair infected files</b>, any infected files are not moved to the Quarantine, even if you choose <b>Quarantine files that cannot be repaired</b>.</p> <p><b>Warning!</b> The software asks whether you want to repair an infected file. If you do not repair the file, it is left on the computer. If you choose <b>Automatically repair infected files</b>, and if you do not choose <b>Quarantine files that cannot be repaired</b>, any infected files are deleted.</p>

## Mac Global Scan Options

This policy option lets you specify the files or folders that you want Auto-Protect, scheduled scans, and manual scans to scan. You can choose from the options in the following table.

**Table 443: General scan details**

Global scan option	Description
<b>Scan everywhere</b>	All files and folders on the client computer are scanned.
<b>Scan only in the following folders</b>	Lets you specify the files or folders that you want Auto-Protect, scheduled scans, and manual scans to scan.
<b>Scan everywhere except in specified folders</b>	<p>Lets you create an Exceptions policy for Mac client computers. This policy lets you omit specified files or folders from Auto-Protect scans, scheduled scans, and manual scans.</p> <p><b>Note:</b> You must choose this option and then create an Exceptions policy.</p> <p><b>Note:</b> <a href="#">Creating exceptions for Virus and Spyware scans</a></p>

The use of symbolic links (symlinks) when you define paths for **Scan only in the following folders** and **Scan everywhere except in specified folders** is not supported. For example, /var is a symbolic link representing /private/var. If you define a path with /var, the scan does not work as expected. You must define the file path with /private/var/.

## Mac Global Scan Options: Files and folders to scan

You can specify files and folders to include in Auto-Protect scans and scheduled scans for Mac clients.

### NOTE

Folder paths for Mac clients must be denoted by using a forward slash. A backward slash is used for Windows paths.

You can add files or folders to the list to include, or you can remove them.

**Table 444: Folders to scan**

Folder option	Description
Prefix variable	<p>You can specify a common top-level location on the client.</p> <p>You can choose from the following prefix variables:</p> <ul style="list-style-type: none"><li>• <b>HOME</b> The home folder for the user that is currently logged on. A home folder path is typically /Users/username, where username matches the user name of the logged on user.</li><li>• <b>APPLICATION</b> The system application folder, which is /Applications.</li><li>• <b>LIBRARY</b> The folder for common system libraries, which is /Library.</li></ul>
File or folder	<p>You can specify files or folders inside the prefix variable. If you did not choose a prefix variable, then enter the full file path.</p> <p>The use of symbolic links (symlinks) in this field is not supported. For example, /var is a symbolic link representing /private/var. If you define a path with /var, the scan does not work as expected. You must define the file path with /private/var/.</p>

## Download Protection: Download Insight

You can enable or disable Download Insight and change how sensitive Download Insight is to potentially malicious files. You can also specify the additional criteria that Download Insight uses when it makes a decision about a file. Use these settings to help control the number of false positive detections.

### NOTE

A lock icon appears next to some options. Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

**Table 445: Download Insight settings**

Option	Description
<b>Enable Download Insight to detect potential risks in downloaded files based on file reputation</b>	<p>Enables or disables Download Insight. Download Insight can detect a malicious file or potentially malicious file when a user tries to download the file from a browser or a text messaging client.</p> <p>Click the icon to lock or unlock this option on client computers.</p> <p>Download Insight requires Auto-Protect. If Auto-Protect is disabled and Download Insight is enabled, Download Insight cannot function. On the client, the status details indicate the Download Insight malfunction.</p>
<b>Specify the malicious file sensitivity</b>	<p>Sets the sensitivity level for Download Insight detection of malicious files. You might want to adjust the slider to change the overall number of detections as well as the number of false positive detections.</p> <p>Click the icon to lock or unlock this option on client computers.</p> <p><b>Note:</b> If Download Protection is not installed, Download Insight runs on the client at level 1. Any level that you set in the policy is not applied. The user also cannot adjust the sensitivity level.</p> <p>Download Insight determines that a downloaded file might be a risk based on evidence about the file's reputation. Symantec collects information about files to determine their reputation and makes the information available to Download Insight. The slider indicates a range of reputations, from most likely to be malicious to least likely to be malicious.</p> <p>You can adjust the slider to change the reputation level at which files are considered malicious or unproven.</p> <p>When you set the sensitivity level higher, Download Insight detects more files as malicious and considers fewer files as unproven. At higher levels, Download Insight returns more false positive detections. Only the files with the best reputations are allowed.</p> <p>At lower sensitivity levels, Download Insight detects fewer files as malicious and returns fewer false positive detections. However, more files are considered unproven.</p> <p><b>Note:</b> Move the slider to view a description of each level. Each description provides information about how the level allows or blocks files and its potential false positive rate.</p> <p>Use the <b>Actions</b> tab to set the action that Download Insight takes on malicious files and unproven files.</p>
<b>Also detect files as malicious based on their use in the Symantec Community</b>	<p>Sets the additional requirements for the downloaded files that have the reputations that are higher than the configured sensitivity setting. The files are considered unproven but are detected as malicious if they meet the additional requirements.</p> <p>The additional requirements enable Download Insight to consider file usage in the Symantec Community. Files that are used by fewer users might be potentially more harmful. Files that have recently appeared in the Symantec Community also might be more potentially harmful.</p> <p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Files with x or fewer users</b> Specifies the maximum number of users who use the file. The client detects any downloaded files that are used by fewer than the specified number of users.</li> <li>• <b>Files known by users for x or fewer days</b> Specifies the maximum number of days that the file has been known in the Symantec community. The client detects any downloaded files that are known by Symantec for less than the number of specified days.</li> </ul> <p><a href="#">Preventing ransomware attacks with Download Insight</a></p>

Option	Description
<b>Automatically trust any file downloaded from an Internet or intranet site</b>	<p>Not supported when Download Protection is not installed on the client computer.</p> <p>By default, Download Insight does not examine any files that users download from a trusted Internet or intranet site. You configure trusted sites and trusted local intranet sites on the <b>Windows Control Panel &gt; Internet Options &gt; Security</b> tab.</p> <p>When this option is enabled, Symantec Endpoint Protection allows any file that a user downloads from one of the trusted sites. After the file is downloaded, other protection features can detect and take action on the file if necessary.</p> <p>Symantec Endpoint Protection checks for updates to the list when you re-enable <b>Automatically trust any file downloaded from Internet or intranet site</b> after it has been disabled. Symantec Endpoint Protection also checks for updates to the Internet Options trusted sites list at user logon and every four hours.</p> <p>You can also create exceptions for specific trusted Web domains.</p> <p>Download Insight recognizes explicitly configured trusted sites only. Wildcards are allowed, but non-routable IP address ranges are not supported. For example, Download Insight does not recognize 10.*.* as a trusted site. Download Insight also does not support the sites that the <b>Internet Options &gt; Security &gt; Automatically detect intranet network</b> option discovers.</p> <p><b>Note:</b> If you disable Download Insight and this option appears grayed out, scans continue to use this option if it is enabled.</p>

## Download Protection: Actions

You can specify how Download Insight responds to malicious file detections and unproven file detections. You can change what level of file reputation Download Insight uses to determine if a file is malicious or unproven by adjusting the sensitivity slider.

### NOTE

A lock icon appears next to some options. Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

**Table 446: Download Insight actions**

Option	Description
<b>Malicious files</b>	<p>Configures the actions for the detections that Download Insight determines are malicious. You can configure a first action to take and a second action to take if the first action fails. The options available for <b>If first action fails</b> are based on the current selection for <b>First action</b>.</p> <p>Click the icon to lock or unlock this option on client computers.</p> <p><b>You can specify the following actions:</b></p> <ul style="list-style-type: none"> <li>• <b>Quarantine risk</b> Tries to move the file to the Quarantine on the client computer as soon as it is detected. When notifications are enabled, Symantec Endpoint Protection displays a notification on the computer. The user can undo the quarantine action, and the file is considered "user allowed". If the file is moved to the Quarantine, the user cannot run the file.</li> <li>• <b>Delete risk</b> Tries to delete the file. The file is permanently deleted and cannot be recovered from the recycle bin. Download Insight displays a notification about the detection but the user cannot undo the action. If the client cannot delete the file, detailed information about the action appears in the <b>Notifications</b> window and the System log.</li> <li>• <b>Leave alone (log only)</b> Allows access to the file and logs the event. Use this option to take manual control of how the client handles a detection. You can specify an action for the detection in the Risk log.</li> </ul>
<b>Unproven files</b>	<p>Configures an action for Download Insight to take when it detects an unproven file. Click the icon to lock or unlock this option on client computers.</p> <p><b>The actions for unproven files are the same as for malicious files (Quarantine risk, Delete risk, Leave alone (log only)), with the following two additional possible actions:</b></p> <ul style="list-style-type: none"> <li>• <b>Prompt</b> Prompts the user to allow or block the downloaded file. If the user allows a file, the file is considered "user allowed".</li> <li>• <b>Ignore</b> Allows the file on the client computer silently. Download Insight does not display a notification.</li> </ul>

## Download Protection: Notifications

You can specify whether or not notifications appear on client computers for Download Insight detections. You can customize the text. The notification includes information about the security risk detected.

### NOTE

A lock icon appears next to some options. Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

**Table 447: Notifications options**

Option	Description
<b>Display a notification message on the infected computer</b>	Enables or disables the display of a notification message on an infected computer when Download Protection makes a detection. Click the icon to lock or unlock this option on client computers. When this option is enabled, you can modify the default message that appears if the user allows the file.

## Global Scan Options

You can configure options that apply to all virus and spyware scans.

### NOTE

A lock icon appears next to some options. Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

**Table 448: Global scan options**

Option	Description
<b>Enable Insight for</b>	Insight allows scans to skip digitally signed files and trusted files. You can configure the level of trust to use when Insight uses reputation data to skip files. If you select <b>Symantec and Community Trusted</b> , scans skip more files (less secure). If you select <b>Symantec Trusted</b> , scans skip fewer files (more secure). When scans skip files, the scan performance might improve. Click the icon to lock or unlock this option on client computers.
<b>Enable Bloodhound heuristic virus detection</b>	Bloodhound isolates and locates the logical regions of a file to detect a high percentage of unknown viruses. Bloodhound then analyzes the program logic for virus-like behavior. Click the icon to lock or unlock this option on client computers. You can set the detection level to either of the following options: <ul style="list-style-type: none"> <li>• <b>Automatic</b> This setting is the default. Bloodhound uses advanced heuristics to make detections. It also uses some experimental heuristics if detection submissions are enabled on clients.</li> <li>• <b>Aggressive</b> Increases the sensitivity of the automatic Bloodhound Detection. If you select this level, you are likely to see more false positive detections. This option is only recommended for advanced users.</li> </ul>
<b>Ask for a password before scanning a mapped network drive</b>	Specifies whether or not clients prompt users for a password when the client scans network drives. The default password is symantec. You can change the password by clicking <b>Change Password</b> and setting the password. The password is saved with both MD5 and SHA-256 hashing. Symantec Endpoint Protection 12.1.2 clients use SHA-256 hashing. MD5 is used for earlier clients.
<b>Display notifications about detections and remediations when the user logs on</b>	Shows notifications about Auto-Protect and scheduled scan detections and remediations when the user logs on.

[Modifying global scan settings](#)

## Edit Folders

You can use this dialog box to select specific folders to be scanned rather than scanning all the files on the computer.

**Table 449: Folder options**

Option	Description
Scan all folders and drives	Specifies that all folders are to be scanned
Scan selected folders	Specifies that all the checked folders are scanned. You select Windows folders, rather than absolute folder paths. Client computers in your security network might use different paths to these folders.

## File Extensions

When you configure a scan for selected file extensions, you can add new extensions to the list or remove any extensions from the list. By default, the client scans all extensions.

Scheduled and on-demand scans always scan container file extensions, such as .zip, regardless of the extensions that you select to scan. You can disable the **Scan files inside compressed files** option in the **Advanced Scanning Options** dialog box to disable scans of container file extensions.

**Table 450: File extensions options**

Option	Description
<b>Use Defaults</b>	Returns the extensions list to its default state. Any extensions that you added are removed, and any default extensions that you removed are added.
<b>Add Common Programs</b>	Selects all extensions for common programs.
<b>Add Common Documents</b>	Selects all extensions for common documents.

**Table 451: Recommended file extensions for scanning**

File extension	Description
CHM	HTML compiled help file for Microsoft Windows
386	Driver
ACM	Driver; audio compression manager
ACV	Driver; audio compression or decompression manager
ADT	ADT file; fax
AX	AX file
BAT	Batch
BTM	Batch
BIN	Binary
CLA	Java Class
CMD	Command file
COM	Executable
CPL	Applet Control Panel for Microsoft Windows
CSC	Corel Script
CSH	UNIX Shell script
DLL	Dynamic Link Library

File extension	Description
DOC	Microsoft Word
DOT	Microsoft Word
DRV	Driver
EXE	Executable
HLP	Help file
HTA	HTML application
HTM	HTML
HTML	HTML
HTT	HTML
INF	Installation script
INI	Initialization file
JPEG	Graphics file
JPG	Graphics file
JS	JavaScript
JSE	JavaScript Encoded
JTD	Ichitaro
MDB	Microsoft Access
MP?	Microsoft Project
MSO	Microsoft Office 2000
OBD	Microsoft Office binder
OBT	Microsoft Office binder
OCX	Microsoft object that links and embeds custom control
OV?	Overlay
PDF	Adobe Portable Document Format
PIF	Program information file
PL	PERL program source code (UNIX)
PM	Presentation Manager Bitmaps Graphics
POT	Microsoft PowerPoint
PPT	Microsoft PowerPoint
PPS	Microsoft PowerPoint
RTF	Rich Text Format document
SCR	Fax, screensaver, snapshot, or script for Farview or Microsoft Windows
SH	Shell Script (UNIX)
SHB	Corel Show Background file
SHS	Shell scrap file
SMM	Lotus AmiPro
SYS	Device driver
VBE	VESA BIOS (Core Functions)
VBS	VBScript
VSD	Microsoft Office Visio



File extension	Description
VSS	Microsoft Office Visio
VST	Microsoft Office Visio
VXD	Virtual device driver
WSF	Windows Script File
WSH	Windows Script Host Settings File
XL?	Microsoft Excel
XL??	Microsoft Excel
ACCD?	Microsoft Office Access
DOC?	Microsoft Office Word
DOT?	Microsoft Office Word
PP?	Microsoft Office PowerPoint
PP??	Microsoft Office PowerPoint

## Risk Tracer

Risk Tracer identifies the source of network share-based virus infections on your client computers.

### NOTE

A lock icon appears next to **Enable Risk Tracer**. Click the icon to lock or unlock Risk Tracer settings on client computers. When you lock the settings, you prevent user changes.

Risk Tracer does not block any attacking IP addresses. The option to automatically block IP addresses is enabled by default in the Firewall policy.

**Table 452: Risk Tracer options**

Option	Description
<b>Enable Risk Tracer</b>	<p>Enables or disables Risk Tracer</p> <p>Click the icon to lock or unlock Risk Tracer options on client computers.</p> <p>When Auto-Protect detects an infection, it determines if the infection originated locally or remotely.</p>
<b>Resolve the source computer IP address</b>	<p>If this option is disabled, the Symantec Endpoint Protection client looks up and records only the computer's NetBIOS name. If this option is enabled, the client tries to get an IP address for the known NetBIOS name.</p> <p><b>If the infection came from a remote computer, Risk Tracer can do the following actions:</b></p> <ul style="list-style-type: none"> <li>• Look up and record the computer's NetBIOS computer name and its IP address.</li> <li>• Look up and record who was logged on to the computer at delivery time.</li> <li>• Display the information in the Risk properties dialog box.</li> </ul>

Option	Description
<b>Poll for network sessions every &lt;number&gt; milliseconds</b>	<p>Enables or disables polling for network sessions</p> <p>Lower values use greater amounts of CPU and memory. Lower values also increase the possibility that the client can record the network session information before the threat can turn off network shares.</p> <p>Higher values decrease system overhead, but also decrease Risk Tracer's ability to detect the source of the infections.</p> <p>Risk Tracer polls at the specified interval for network sessions, and then caches this information as a remote computer secondary source list. This information maximizes the frequency with which Risk Tracer can successfully identify the infected remote computer. For example, a risk may close the network share before Risk Tracer can record the network session. Risk Tracer then uses the secondary source list to try to identify the remote computer. You can configure this information in the Auto-Protect Advanced Options dialog box.</p>

Risk Tracer information appears in the Risk Properties dialog box, and is available only for the risk entries that the infected files cause. When Risk Tracer determines that the local host activity caused an infection, it lists the source as the local host.

**Risk Tracer lists a source as unknown when the following conditions are true:**

- It cannot identify the remote computer.
- The authenticated user for a file share refers to multiple computers. This condition can occur when a user ID is associated with multiple network sessions. For example, multiple computers might be logged on to a file sharing server with the same server user ID.

You can record the full list of multiple remote computers that currently infect the local computer. Set the HKEY\_LOCAL\_MACHINE\Software\Symantec\Symantec Endpoint Protection\AV\ProductControl\Debug string value to "THREATTRACER X" on the local client computer. The THREATTRACER value turns on the debug output and the X ensures that only the debug output for Risk Tracer appears. You can also add an L to ensure that the logging goes to the vpdebug.log file. To ensure that the debug window does not appear, add XW.

If you want to experiment with this feature, use the test virus file Eicar.com available from the following URL:

[www.eicar.org](http://www.eicar.org)

## File Cache

You can configure file cache options for Auto-Protect scans of the file system. Auto-Protect uses a file cache so that it remembers the clean files from the last scan. The file cache persists across startups. If the client computer shuts down and restarts, Auto-Protect remembers the clean files and does not scan them.

**Auto-Protect rescans the files in the following situations:**

- The client computer downloads new definitions.
- Auto-Protect detects that the files might have changed when Auto-Protect was not running.

You can disable the file cache if you always want Auto-Protect to scan every file. If you disable the file cache, you might impact the performance of your client computers.

### NOTE

A lock icon appears next to **Enable file cache**. Click the icon to lock or unlock file cache settings on client computers. When you lock the settings, you prevent user changes.

**Table 453: File cache options**

Option	Description
<b>Enable file cache</b>	Enables or disables the file cache File caching decreases Auto-Protect's memory usage and can help improve Auto-Protect scan performance. You can disable this option for troubleshooting. If you disable this option, when the client computer restarts, Auto-Protect rescans all files. Click the icon to lock or unlock file cache options on client computers.
<b>Use the default file cache size</b>	Applies only to 11.0 clients. Uses the default file cache size when file caching is enabled. The default file cache size is based on typical file usage patterns and is determined dynamically. 12.1 clients handle the cache size automatically.
<b>Use a custom file cache size</b>	Applies only to 11.0 clients. Uses a specified number of file cache entries rather than the default size You can specify the number of custom file cache entries to include. This option is useful for file servers or Web servers on which you want to cache a large number of files. 12.1 clients handle the cache size automatically.
<b>Rescan cache when new definitions load</b>	Enables Auto-Protect to rescan the cache when the client computer receives new definitions You can disable this option to improve client computer performance.

## Auto-Protect: Scan Details

Use the **Scan Details** tab to configure scanning and drive type options for Auto-Protect scans of files and processes.

### NOTE

A lock icon appears next to some options. Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

Use an Exceptions policy to specify scan exclusions for files or folders.

**Table 454: Auto-Protect scan detail options**

Option	Description
<b>Enable Auto-Protect</b>	<p>Enables or disables Auto-Protect for the file system By default, Auto-Protect is enabled.</p> <p><b>If you disable Auto-Protect, you automatically make the following changes to the protection on your client computers:</b></p> <ul style="list-style-type: none"> <li>• Download Insight does not function even if Download Insight is enabled.</li> <li>• SONAR does not detect heuristic threats. SONAR detection of system changes or host file changes, however, continues to function.</li> </ul>
<b>Scanning</b>	<p>You can scan all file types or only files with selected extensions.</p> <ul style="list-style-type: none"> <li>• <b>Scan all files</b> Scans all files on the computer, regardless of type.</li> <li>• <b>Scan only selected extensions</b> Scans only the files that have certain extensions. You can add more extensions for programs and documents, if you have files that use the extensions that are not already in the list. You can also reset this option to its default value.</li> <li>• <b>Determine file types by examining file contents</b> Scans a specific, configurable group of the file extensions that contain executable code, and all .exe and .doc files. The Symantec Endpoint Protection client reads each file's header to determine its file type. It scans .exe and .doc files even if a virus changes the file extensions for the .exe and the .doc files. This option is disabled by default.</li> <li>• <b>Select Extensions</b> Specifies that only certain file extensions should be included in the scan. You can add or remove file extensions to scan. Only the file extensions that you specify are scanned. The client does not scan any files that have extensions that are not in the list. <b>Note:</b> If you want to exclude files or folders from scans, create an exception.</li> <li>• <b>Scan for security risks</b> This option is enabled by default. On Windows clients and Linux clients, you can disable Auto-Protect scanning for security risks. You can temporarily disable Auto-Protect scanning of security risks if a detection of a security risk could compromise a computer's stability. However, Symantec recommends that you add an exception to the Exceptions policy instead of disabling this option. If you disable this option, scheduled and on-demand scans continue to detect the risk. <b>Note:</b> This option has no effect on the computers that run earlier versions of the client.</li> <li>• <b>Advanced Scanning and Monitoring</b> Provides options for triggering automatic scans and other advanced options.</li> </ul>

Option	Description
Network Settings	<p><b>Network settings provides the following options for scanning files on remote computers:</b></p> <ul style="list-style-type: none"> <li>• <b>Scan files on remote computers</b> Enables or disables scanning on network drives. If you disable this option, you might improve client computer performance.</li> <li>• <b>Only when files are executed</b> By default, Auto-Protect scans files on remote computers only when file are executed. You can disable this option to scan all files on remote computers, but you might impact your client computer performance.</li> <li>• <b>Network Settings</b> When scanning is enabled on network drives, Auto-Protect scans files when a client computer or a server accesses them from a server. When network scanning is enabled, you can also enable Auto-Protect to trust remote versions of Auto-Protect and to use a network cache.</li> </ul>

## Advanced Scanning and Monitoring

You can configure the Symantec Endpoint Protection client to scan for particular actions and to watch files for suspicious behavior.

### NOTE

A lock icon appears next to some options. Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

**Table 455: Advanced scanning and monitoring details**

Group or Option	Description
<b>Scan Files When</b>	<p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Scan when a file is accessed or modified</b> Scans the files when they are written, opened, moved, copied, or run Use this option for more complete file system protection. This option might affect performance because Auto-Protect scans files during all types of file operations. You can lock or unlock this option to prevent or allow user changes.</li> <li>• <b>Scan when a file is modified</b> Scans the files when they are written, modified, or copied. Use this option for slightly faster performance, because Auto-Protect scans files only when they are written, modified, or copied.</li> <li>• <b>Scan when a file is backed up</b> Scans a file during backup if another process tries to write to the file during the backup. The backup process only reads the files during backup, so the backup process itself does not initiate the scan. If you disable this option, Auto-Protect does not scan any file during a backup. The client scans the files that it restores from a backup, however, regardless of this setting. You can lock or unlock this option to prevent or allow user changes.</li> <li>• <b>Do not scan files when trusted processes access the files</b> Skips files that are accessed by Windows Search indexer and other processes that Symantec Endpoint Protection determines are safe. Use the custom list if you want to control which processes can skip files. You can lock or unlock this option to prevent or allow user changes.</li> <li>• <b>Enable custom list</b> Only available when <b>Do not scan files when trusted processes access the files</b> is enabled. Use <b>Customize process list</b> to specify the processes that you consider safe processes. Enter the file name of the process; do not include the path. Scans skip the files that are accessed by the processes in this list as well as by the processes that Symantec trusts.</li> </ul>
<b>Floppy Settings</b>	<p>You can lock or unlock this option to prevent or allow user changes.</p> <p><b>Floppy settings provides the following options:</b></p> <ul style="list-style-type: none"> <li>• <b>Check floppies for boot viruses when accessed</b> Enables or disables floppy disk scanning for boot viruses when the floppies are accessed for data. This option is enabled by default.</li> <li>• <b>When a boot virus is found:</b> Sets the action to take when a boot virus is found, either clean it from the boot record, or log it and leave it alone. If you select Leave alone (log only), an alert is sent when a virus is detected, but no action is taken. Use this option if you want the computer user to control the virus cleaning and handling process.</li> </ul>
<b>Other Options</b>	<p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Always delete newly created infected files</b> Enable this option to delete a new file that is infected regardless of the action that is configured for the type of risk. This setting does not apply to Auto-Protect detections of existing files that contain viruses. Auto-Protect does not delete infected files that already exist on the client computer unless the configured action is <b>Delete</b>. You can lock or unlock this option to prevent or allow user changes.</li> <li>• <b>Always delete newly created infected security risks</b> This option is only available when <b>Always delete newly created infected files</b> is enabled. Enable this option to delete a newly created file that contains a security risk regardless of the action that is configured for the type of risk. This setting does not apply to Auto-Protect detections of existing files that contain security risks. Auto-Protect does not delete security risks that already exist on the client computer unless the configured action is <b>Delete</b>.</li> </ul>

## Quarantine: General

You can use this tab to set the options for the local quarantine for Windows clients.

**Table 456: Quarantine options**

Option	Description
<b>When New Virus Definitions Arrive</b>	<p>Specifies what happens when a computer receives new virus and security risk definitions</p> <ul style="list-style-type: none"><li>• <b>Automatically repair and restore files in Quarantine silently</b> If the new definitions include repairs for quarantined files, Symantec Endpoint Protection repairs the files. The client also restores the files to their previous location without notifying the user.</li><li>• <b>Repair files in Quarantine silently without restoring</b> If the new definitions include a repair for quarantined files, the client repairs the files but does not restore them to their previous location.</li><li>• <b>Prompt user</b> The user is prompted to decide whether or not to try to repair quarantined files.</li><li>• <b>Do nothing</b> The client does not try to repair quarantined files.</li></ul>
<b>Local Quarantine Options</b>	<p>Specifies the folder where files are quarantined You can select the default folder or browse to any other folder that you want to use. <b>You can also the following expansion parameters:</b></p> <ul style="list-style-type: none"><li>• %COMMON_APPDATA% Folder that contains application data for all users, and is not user-specific. A typical path is C:\ProgramData.</li><li>• %PROGRAM_FILES% The <b>Program Files</b> folder. A typical path is C:\Program Files. On a 64-bit system, Symantec Endpoint Protection uses the 64-bit and 32-bit system locations. The 32-bit system location is C:\Program Files (x86).</li><li>• %PROGRAM_FILES_COMMON% Folder that contains the components that are shared across applications. A typical path is C:\Program Files\Common Files. On a 64-bit system, Symantec Endpoint Protection uses the 64-bit and 32-bit system locations. The 32-bit system location is C:\Program Files (x86)\Common Files.</li><li>• %COMMON_PROGRAMS% Folder that contains the common program groups that appear on the <b>Start</b> menu for all users. A typical path is C:\ProgramData\Microsoft\Windows\Start Menu\Programs.</li><li>• %COMMON_STARTUP% Folder that contains the programs that appear in the Startup folder for all users. A typical path is C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup.</li><li>• %COMMON_DESKTOPDIRECTORY% Folder that contains the files and folders that appear on the desktop of all users. A typical path is C:\Users\Public\Desktop.</li><li>• %COMMON_DOCUMENTS% Folder that contains the documents that are common to all users. A typical path is C:\Users\Public\Documents.</li><li>• %SYSTEM% The Windows System folder. This path is typically C:\Windows\System32.</li><li>• %WINDOWS% The Windows folder. This path is typically C:\Windows.</li></ul>

Option	Description
<b>Quarantined Items</b> (removed in 14.3 RU2)	<p><b>Note:</b> Version 14 and later does not include the Quarantine Server and Quarantine Console. You can install these tools from the installation disc in an earlier version.</p> <p><b>Allow client computers to automatically submit quarantined items to a Quarantine Server</b> (default is disabled): Specifies whether or not client computers automatically submit quarantined items to an existing Central Quarantine Server in your environment. You can then use this central repository of samples for internal purposes, such as to research offensive (red team) events.</p> <p><b>Configure the following parameters for the Quarantine Server:</b></p> <ul style="list-style-type: none"> <li>• <b>Server name/Port</b> The server name or IP address and the port that is configured for the Quarantine Server. By default, port is 33</li> <li>• <b>Retry</b> By default, this option is 600 seconds.</li> </ul>

## Scheduled scan details for Mac clients

You can specify drives and folders to scan for scheduled scans.

### NOTE

You cannot specify the scan type for Mac clients. Different scan types are available only for Windows clients. Mac clients always run custom scans. If you run an active scan command on a group that includes Mac clients and Windows clients, the Windows clients run the active scan. The Mac clients, however, run a custom scan.

**Table 457: Scheduled scan details**

Option	Description
Scan name	You can enter a name for this scan that lets you identify it easily. The scan name is limited to 128 characters.
Description	You can provide a more detailed description of the scan. The description is limited to 255 characters.
Scan drives and folders	<p>You can specify whether to scan hard drives or removable drives, or both. You can also select which folders to scan.</p> <p><b>Note:</b> If no user is logged on at the time of the scheduled scan of a Home folder, then the scan does not run.</p> <p>You can also enable or disable idle-time scans.</p>

## Administrator-defined Scans: Notifications

You can use this tab to create a message to appear on an infected computer when a virus or a security risk is detected.

Notification messages for the client for Mac appear in the macOS (or Mac OS X) Notification Center. Due to the character limitations of Notification Center, you cannot customize the messages for Mac.



**Table 458: Notifications options**

Option	Description
<b>Display a notification message on the infected computer</b>	Specifies that a message is displayed on an infected computer You can modify the type of information that appears in the message when the client finds a virus or a security risk.
<b>Save a copy as a Scheduled Scan Template</b>	Saves a copy of the message as a template for future messages. <b>Note:</b> This option is only available when you add a scheduled scan for clients that run on Windows computers.

**Table 459: Notification message fields**

Label	Field	Description
<b>Scan type</b>	<b>LoggedBy</b>	The type of scan, on-demand, scheduled, and so on, that detected the virus or security risk.
<b>Event</b>	<b>Event</b>	The type of event, such as "Risk Found."
<b>Security risk detected</b>	<b>SecurityRiskName</b>	The name of the virus or security risk that was found.
<b>File</b>	<b>PathAndFilename</b>	The complete path and name of the file that the virus or the security risk has infected.
<b>Location</b>	<b>Location</b>	The drive on the computer on which the virus or security risk was located.
<b>Computer</b>	<b>Computer</b>	The name of the computer on which the virus or security risk was found.
<b>User</b>	<b>User</b>	The name of the user who was logged on when the virus or security risk occurred.
<b>Action taken</b>	<b>ActionTaken</b>	The action that was taken in response to detecting the virus or security risk. This action can be either the first action or second action that was configured.
<b>Date found</b>	<b>DateFound</b>	The date on which the virus or security risk was found.
<b>Status</b>	<b>Status</b>	The date on which the virus or security risk was found. This message variable is not used by default. To display this information, manually add this variable to the message.

## Early Launch Anti-Malware Driver Options

Symantec Endpoint Protection provides an early launch anti-malware (ELAM) driver that works with the Microsoft ELAM driver to protect the computers in your network when they start and before third-party drivers initialize. The settings are supported on Microsoft Windows 8 and Windows Server 2012.

**Table 460: Early launch anti-malware options**

Option	Description
<b>Enable Symantec early launch anti-malware</b>	Enables the Symantec Endpoint Protection early launch anti-malware (ELAM) driver. When this option is enabled, the settings take effect only when the Windows ELAM driver is enabled.
<b>When a potentially malicious driver is detected</b>	<p><b>You can choose one of the following options:</b></p> <ul style="list-style-type: none"><li>• <b>Log the detection as unknown so that Windows allows the driver to load</b> This log-only option configures the Symantec Endpoint Protection early launch anti-malware driver to report bad or bad critical drivers as unknown drivers to Windows. Symantec Endpoint Protection logs the detection as a bad or bad critical driver, and then Windows uses the action in its policy for unknown drivers. By default, Windows allows unknown drivers to load. You might select this option if you get false positive detections that block important drivers.</li><li>• <b>Use the default Windows action for the detection</b> You use the Windows Group Policy editor to view and modify the Windows ELAM settings. See your Windows documentation for more information.</li></ul>

## Actions

You can configure actions for administrator-defined scans and for Auto-Protect.

As of 14.3 RU1, configuring the actions for detections is deprecated for the Linux client.

### NOTE

A lock icon appears next to some options. Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

**Table 461: Actions options**

Detection type	Action options
<b>Malware</b>	<p>You can configure a first action to take and a second action to take if the first action fails.</p> <p><b>Note:</b> By default, Auto-Protect automatically deletes newly created or saved infected files regardless of the action options that you specify here.</p> <p>You can lock or unlock action options to prevent or allow user changes.</p> <p><b>Actions for viruses include the following actions:</b></p> <ul style="list-style-type: none"> <li>• <b>Clean risk</b> (default first action): Tries to repair a file that is infected with a virus. This action has no effect on Trojan horses or worms.</li> <li>• <b>Quarantine risk</b> (default second action): Tries to move the infected file to the Quarantine on the infected computer as soon as it is detected. After an infected file is moved to the Quarantine, a user on that client computer cannot run the file. However, the user can select an action for the file in the Quarantine. For example, the user can specify that the client should clean the file and move the file back to its original location.</li> <li>• <b>Delete risk:</b> Tries to delete the file. Use this option only if you can replace the infected file with a virus-free backup copy. The file is permanently deleted and cannot be recovered. If the client cannot delete the file, detailed information about the action appears in the <b>Notifications</b> window and the System log.</li> <li>• <b>Leave alone (log only):</b> Denies the access to the file, displays a notification, and logs the event. You can use the log to take manual control of how the client handles a virus. Open the Risk log, right-click the name of the file, and select one of the following actions: <b>Clean</b> (viruses only), <b>Delete Permanently</b>, or <b>Move To Quarantine</b>. A user on the client computer can also specify an action for the risk in the Risk log. <a href="#">Risk logs and quick reports</a></li> </ul>
<b>Security Risks</b>	<p>You can lock or unlock action options to prevent or allow user changes.</p> <p><b>Note:</b> By default, Auto-Protect automatically deletes newly created or saved security risks regardless of the action options that you specify here.</p> <p><b>You can configure security risk actions as follows:</b></p> <ul style="list-style-type: none"> <li>• Configure the same actions to take for all security risks.</li> <li>• Configure the same actions for a whole category of security risks.</li> <li>• Configure individual security risk exceptions to the actions that you set for specific categories. The <b>Override actions configured for Security Risks</b> option is disabled by default.</li> </ul> <p>You can configure a first action to take and a second action to take if the first action fails.</p> <p><b>Actions for security risks include the following:</b></p> <ul style="list-style-type: none"> <li>• <b>Quarantine risk</b> (default first action): Tries to move any infected files to the Quarantine on the infected computer as soon as the security risk is detected or completes its installation. The client removes or repairs any side effects of the risk. Side effects include additional registry keys, modified registry key values, additions to .ini or .bat files, or extra entries in hosts files. Side effects also include errors in a system driver or the effects of a rootkit. You can restore the security risk items that are quarantined to their original state on the computer. In some instances, you might need to restart the computer to complete the removal or repair.</li> <li>• <b>Delete risk</b> (default second action): Tries to delete security risk files. Use this option only if you can replace the files with a clean backup copy. You cannot recover permanently deleted files. Use this action with caution. The deletion of security risks can cause applications to lose functionality. If the client cannot delete files, detailed information about the actions appears in the <b>Notifications</b> window and the System log.</li> <li>• <b>Leave alone (log only):</b> The risk is left alone and its detection is logged. Use this option to take manual control of how the client handles a security risk. When you select this action, by default Symantec Endpoint Protection automatically deletes the newly created or saved files that are security risks. You can use the Risk log in the console to specify the action for the logged risk. Users on client computers can use the logs to specify the action as well.</li> </ul>
	<p>You can also lock exceptions so that users cannot create their own security risk exceptions for scans. 867</p> <p><b>Note:</b> In some instances, you might unknowingly install an application that includes a security risk such as adware or spyware. If Symantec has determined that blocking the risk does not harm the computer, then by default the client blocks the risk. If the block action might make the computer unstable, the client waits after the application installation. The client then performs the configured action on the</p>

---

## Edit scheduled scan: Scan details

You can specify folders and file types for scheduled scans.

### NOTE

You cannot specify the scan type for Linux clients. Different scan types are available only for Windows clients. Linux clients always run custom scans. If you run an active scan command on a group that includes Linux clients and Windows clients, the Windows clients run the active scan. The Linux clients, however, ignore the command and do not run a scan.

**Table 462: Scheduled scan details**

Option	Description
<b>Scan name</b>	Specifies the name you want to use for the scan. For Administrator on-demand scans, the scan name is <b>Administrator On-demand Scan</b> , which cannot be changed.
<b>Description</b>	Provides a description of the scan for future reference. For Administrator on-demand scans, the description is a default on-demand scan description, which cannot be changed.
<b>Folder types</b>	Specifies the folders on which to run the scan. This setting is useful to save scanning time and computer resources.
<b>File types</b>	Specifies the types of files be scanned. You can scan all files or limit the scan to files with specific extensions.
<b>Specify whether files inside compressed files should be scanned</b>	Lets you limit scanning of compressed files. Also lets you specify how many levels deep to scan inside compressed files.
<b>Additional options</b>	Lets you choose whether to scan for security risks. Scanning for security risks slows the scan down, but increases security. The default is to scan for security risks.

## Linux Global Scan Options

(as of 14.3 RU3)

You can configure options that apply to all virus and spyware scans on Linux devices.

[Modifying global scan settings](#)

**Table 463: Linux Global Scan Options**

Option	Description
<b>Total Cloud Protection</b>	If enabled, then virus and spyware features use the cloud to evaluate files. Cloud content includes the entire set of virus and spyware definitions as well as the latest information that Symantec has about files and potential threats.
<b>Bloodhound Detection Settings</b>	<p>Bloodhound isolates and locates the logical regions of a file to detect a high percentage of unknown viruses. Bloodhound then analyzes the program logic for virus-like behavior. Check <b>Enable Bloodhound heuristic virus detection</b> to enable it on your Linux devices. You can set the detection level to either of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Automatic</b> This setting is the default. Bloodhound uses advanced heuristics to make detections. It also uses some experimental heuristics if detection submissions are enabled on clients.</li> <li>• <b>Aggressive</b> Increases the sensitivity of the automatic Bloodhound Detection. If you select this level, you are likely to see more false positive detections. This option is only recommended for advanced users.</li> </ul>

## Linux Auto-Protect: Advanced Scanning and Monitoring

You can configure the Symantec Endpoint Protection client to scan for particular actions. You can also fine-tune scans that run on compressed files.

### NOTE

A lock icon appears next to some options. Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

**Table 464: Advanced scanning and monitoring details**

Group or Option	Description
<b>Scan Files When</b>	<p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Scan when a file is accessed or modified</b> Scans the files when they are written, opened, moved, copied, or run Use this option for more complete file system protection. This option might affect performance because Auto-Protect scans files during all types of file operations. You can lock or unlock this option to prevent or allow user changes.</li> <li>• <b>Scan when a file is modified</b> Scans the files when they are written, modified, or copied. Use this option for slightly faster performance, because Auto-Protect scans files only when they are written, modified, or copied.</li> </ul>
<b>Scanning Compressed Files</b>	<p>Lets you limit scanning of compressed files. Also lets you specify how many levels deep to scan inside compressed files. You can lock or unlock this option to prevent or allow user changes.</p>

## Linux Auto-Protect: Scan Details

Use the **Scan Details** tab to configure scanning and drive type options for Auto-Protect scans of files and processes.

Use an Exceptions policy to specify scan exclusions for extensions or folders.

**Table 465: Auto-Protect scan detail options**

Option	Description
<b>Enable Auto-Protect</b>	Enables or disables Auto-Protect for the file system By default, Auto-Protect is enabled. You can lock or unlock this option to prevent or allow user changes.
<b>Scanning</b>	<p>You can scan all file types or only files with selected extensions.</p> <p><b>File types</b> The following options are available:</p> <ul style="list-style-type: none"> <li>• <b>Scan all files</b> Scans all files on the computer, regardless of type.</li> <li>• <b>Scan only selected extensions</b> Scans only the files that have certain extensions. You can add more extensions for programs and documents, if you have files that use the extensions that are not already in the list. You can also reset this option to its default value.</li> <li>• <b>Select Extensions</b> Specifies that only certain file extensions should be included in the scan You can add or remove file extensions to scan. Only the file extensions that you specify are scanned. The client does not scan any files that have extensions that are not in the list.</li> </ul> <p><b>Note:</b> If you want to exclude files or folders from scans, create an exception.</p> <p><b>Removable media</b> This option is enabled by default.</p> <p><b>Additional options</b> Additional options include the following:</p> <ul style="list-style-type: none"> <li>• <b>Scan for security risks</b> This option is enabled by default.</li> <li>• <b>Advanced Scanning and Monitoring</b> Provides options for triggering automatic scans and other advanced options.</li> </ul>
<b>Network Settings</b>	<ul style="list-style-type: none"> <li>• <b>Scan files on remote computers</b> Enables or disables scanning on network drives. If you disable this option, you might improve client computer performance.</li> </ul>

## Linux Auto-Protect: Advanced

You can configure file cache options for Auto-Protect scans of the file system. Auto-Protect uses a file cache so that it remembers the clean files from the last scan. The file cache persists across startups. If the client computer shuts down and restarts, Auto-Protect remembers the clean files and does not scan them again.

### Auto-Protect rescans the files in the following situations:

- The client computer downloads new definitions.
- Auto-Protect detects that the files might have changed when Auto-Protect was not running.

You can disable the file cache if you always want Auto-Protect to scan every file. If you disable the file cache, you might impact the performance of your client computers.

### NOTE

A lock icon appears next to **Enable file cache**. Click the icon to lock or unlock file cache settings on client computers. When you lock the settings, you prevent user changes.

**Table 466: File cache options**

Option	Description
<b>Enable file cache</b>	Enables or disables the file cache. You can disable this option for troubleshooting. Click the icon to lock or unlock file cache options on client computers. File caching decreases Auto-Protect's memory usage and can help you to track problems. Auto-Protect adds a 16-byte entry to the cache index, which remains until Auto-Protect detects a change to the file.
<b>Use the default file cache size</b>	Uses the default file cache size when file caching is enabled. The default file cache size is based on typical file usage patterns. The default cache size is a dynamic value based on the Linux system's memory.
<b>Use a custom file cache size</b>	Uses a specified number of file cache entries rather than the default size. You can specify the number of custom file cache entries to include. This option is useful for file servers or Web servers on which you want to cache a large number of files.

## Custom Process List

You can add or edit process names in this list for scans to skip these files. You should only add processes to the list that you know are safe. The list is used in addition to processes that Symantec already trusts as safe. Add the process name without a path name, for example, `foo.exe`.

## SONAR: SONAR

You can change how SONAR handles certain types of detections. You might want to change these settings to reduce the number of false positive detections.

The default settings depend on the type of Virus and Spyware Protection policy that you use. You can use the balanced policy, the high security policy, or the high performance policy.

### NOTE

A lock icon appears next to some options. Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

Table 467: SONAR settings

Option Group	Options	Description
<b>SONAR</b>	<b>Enable SONAR</b>	Enables or disables SONAR. <b>Note:</b> When SONAR is enabled, <b>Enable Suspicious Detection Behavior</b> is on and cannot be turned off.
<b>Scan Details</b>	<b>High risk detection</b> <b>Low risk detection</b>	Configures the action for SONAR detections of heuristic threats. Heuristic threats are categorized as more likely to be malicious (high risk) or less likely to be malicious (low risk). For low risk detections, you can disable any action. SONAR then only detects the applications that are most likely malicious. <b>You can set the following actions:</b> <ul style="list-style-type: none"> <li>• <b>Quarantine</b> Moves or tries to move the file that is associated with the detection to the local Quarantine on the infected computer.</li> <li>• <b>Log</b> Ignores the detection but logs the event.</li> <li>• <b>Remove</b> Terminates the application and deletes it from the computer. Use this action with caution. In some cases, you can cause an application to lose needed functionality.</li> <li>• <b>Disabled</b> Applies to low risk detections only. When you select this option, SONAR does not detect low risk threats.</li> </ul>
	<b>Enable aggressive mode</b>	Lowers the threshold for low risk detections. When this option is enabled, SONAR is more sensitive to low risk detections, however the false positive rate might be higher.
	<b>When detection found</b>	Configures notifications to alert the user when SONAR makes a detection. <b>You can choose the following notifications:</b> <ul style="list-style-type: none"> <li>• <b>Show alert upon detection</b></li> <li>• <b>Prompt before terminating a process</b></li> <li>• <b>Prompt before stopping a service</b></li> </ul>



Option Group	Options	Description
System Change Events	DNS change detected	<p>Configures the action that SONAR takes when it detects a DNS change or a host file change.</p> <p><b>Note:</b> SONAR does not take any action when a process tries to open or access a host file. SONAR takes action when a process modifies a host file.</p> <p>The DNS or host file change settings do not exempt an application from detection by SONAR. SONAR always detects an application if it exhibits suspicious behavior.</p> <p><b>You can configure the following actions:</b></p> <ul style="list-style-type: none"> <li>• <b>Ignore</b> Ignores the detection. This is the default action. Any action other than <b>Ignore</b> might result in many log events in the console and email notifications to administrators.</li> <li>• <b>Prompt</b> Prompts the user to allow or block the change. This action might result in many notifications on your client computers.</li> <li>• <b>Block</b> Blocks the change.</li> </ul> <p><b>Note:</b> If you set the action to <b>Block</b>, you might block important applications on your client computers.</p> <p><b>Note:</b> For example, if you set the action to <b>Block</b> for <b>DNS change detected</b>, you might block VPN clients. If you set the action to <b>Block</b> for <b>Host file change detected</b>, you might block your applications that need to access the host file.</p> <li>• <b>Log</b> Allows the change but creates a log entry for the event. This action might result in large log files.</li>
	Host file change detected	
Suspicious Behavior Detection	Enable Suspicious Behavior Detection	Enables or disables detection of trusted applications that exhibit suspicious behavior. This option is enabled and not configurable when SONAR is enabled.
	High risk detection Low risk detection	<p>Configures the action that SONAR takes when it detects a trusted application that exhibits suspicious behavior. For example, a trusted application might create executable files or download an untrusted driver.</p> <p><b>You can configure the following actions:</b></p> <ul style="list-style-type: none"> <li>• <b>Ignore</b> Ignores the detection.</li> <li>• <b>Prompt</b> Prompts the user to allow or block the application.</li> <li>• <b>Block</b> Blocks the change.</li> <li>• <b>Log</b> Allows the application but creates a log entry for the event.</li> </ul>
Network Settings	Scan files on remote computers	<p>Enables or disables SONAR scans on network drives. SONAR looks for worms such as Salty, which infects network drives. Salty is a type of malware that infects files on Microsoft Windows systems and spreads through removable drives and network shares. Enable this option when you need to scan the file operations that target network drives. Disable this option to increase the clients' performance.</p>

## Application Control and Device Control

### System Lockdown for group name

System lockdown blocks unapproved applications on client computers in a particular group. Unapproved applications are any applications that are not on an approved list. In Allow Mode (Whitelist Mode), only applications on the list are allowed.

In Deny Mode (Blacklist Mode), applications on the list are blocked, and all unapproved applications are allowed. You can set up system lockdown in either allow mode or deny mode.

**Table 468: System lockdown options**

Option	Definition
<b>System Lockdown</b>	<p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Disable System Lockdown</b> Disables system lockdown. Applications are neither blocked nor logged.</li> <li>• <b>Log Unapproved Applications Only</b> Use this option to test applications before you enable system lockdown. In Allow Mode, this option logs each application that is not listed in the approved applications list. In Deny Mode, this option logs each application that is listed in the unapproved applications list.</li> <li>• <b>Enable System Lockdown</b> In Allow mode, blocks any application that is <b>not</b> listed on the approved applications list. In Deny Mode, blocks any application that <b>is</b> listed in the unapproved applications list.</li> </ul>
<b>Application File Lists</b>	<p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Enable Allow Mode</b> This option only appears if you configured Symantec Endpoint Protection Manager to display these modes. In allow mode, system lockdown allows all applications that you specify in file fingerprint and application lists. System lockdown blocks any applications that are not on the list. This option is <b>Enable Whitelist Mode</b> in 14.3 MP1 and earlier.</li> <li>• <b>Enable Deny Mode</b> This option only appears if you configured Symantec Endpoint Protection Manager to display these modes. In deny mode, system lockdown blocks all applications that you specify in file fingerprint or application lists. System lockdown allows any applications that are not in the list. This option is <b>Enable Blacklist Mode</b> in 14.3 MP1 and earlier.</li> <li>• <b>File Fingerprint List</b> A list of approved file fingerprints that you want to allow or block. Use the <b>Add</b> and <b>Remove</b> buttons to manage this list. When you enable system lockdown, you can select <b>Test Before Removal</b> to log the applications on the file fingerprint list as unapproved applications. Applications are allowed to run on your client computers but are logged as unapproved. After you review the Control log, click <b>Remove</b> to remove the file fingerprint lists that you do not want to use.</li> <li>• <b>File Name</b> A list of approved files. Use the Add and Remove options to manage this list. Use the <b>Import</b> option to import a list of application names if you do not want to add application names one at a time. Check <b>Test Before Removal</b> to log the file as an unapproved file. The application is allowed to run on your client computers but is logged as unapproved. After you review the Control log, click <b>Remove</b> to remove the files that you want to block on client computers.</li> </ul>
<b>Notify the user if an application is blocked</b>	<p>When you enable system lockdown, you can notify the user when system lockdown blocks an application.</p> <p>Use <b>Notification</b> to create a custom message that you want the user to see when system lockdown blocks an application.</p> <p>The operating system limits the amount of text that can be displayed in the notification on a client computer. To avoid the truncation of the notification text, you should limit your added text to no more than 120 characters.</p>

Option	Definition
<b>View Unapproved Applications</b>	Displays a list of applications that would be blocked if you enable system lockdown. In the default Allow Mode, the list shows the applications that do not appear on specified file fingerprint or application lists. For the Deny Mode, the list shows the applications that do appear on the specified file fingerprint or application lists. You can review the list to decide which applications you want to add or remove to the system lockdown configuration. You can also check the Control log.

## Unapproved Applications

You can run system lockdown in test mode, or test individual file fingerprints, application name lists, or applications in the configuration. When you test system lockdown, any applications that system lockdown would block are not blocked. The applications are logged as unapproved so that you can check the list. You can then decide whether to add, keep, or remove the file fingerprints, application name list, or specific application.

You can run a test for a few days to a week and then check the unapproved applications list. You can click **Reset Test** to start the test over.

## Add File or Folder Definition

Use this dialog box to specify the file and the settings that are used to match it.

**Table 469: File definition options**

Option	Description
Entity Name to Match	Specifies the folder name and file name. You can use environment variables, wildcards, and registry keys.
Use wildcard matching (* and ? supported)	Matches the file name if the file name uses wildcards. By default, this option is enabled.
Use regular expression matching	Matches the file name if the file name uses regular expressions.
Only match files on the following drive types	Match the files if they are located on one or more of the checked drive types.
Only match files on the following device id type	Match the files only if they are located on the device with the ID that you specified. Or if you used wildcards, match only if they are located on any device of the ID type that you specified. For example, you can type USBSTOR* to specify any USB storage device. You can click Select to select from a list of default device instances and their IDs.

## Application Control: Application Control Rule Sets

Use this page to view and manage application control rule sets for the selected Application and Device Control policy. An application control rule set contains the rules and conditions that monitor for specified files, folders, and processes. You can create or modify collections of rules for the selected policy.

[Hardening Symantec Endpoint Protection \(SEP\) with an Application and Device Control Policy to increase security](#)

**Table 470: Application Control rule sets**

Option	Description
Enabled	Shows whether this collection of rules is in use or not. Uncheck this option to disable the corresponding rule set in the policy.
Rule Sets	The name of a collection of rules for this policy. You can have multiple collections of rules in one policy.
Test/Production	Whether this collection of rules is in Test (log only) mode or in Production mode. Test mode lets you apply this collection of rules to devices without modifying the behavior of those devices. You can then examine the generated log. When you first create a collection of rules for a policy, the mode is Test (log only). To change the mode to Production, under <b>Test/Production</b> for the collection of rules that you want to change, select <b>Production</b> from the drop-down menu.

## Add Application Control Rule Set

Use this dialog to configure options for a collection of rules in an Application Control policy. These rules make up the rule set. For example, you might want to define a rule for all processes, and then additional rules to match for specific processes.

You should define the process definition first, and then add items under the rule for the process.

### NOTE

If you create a custom rule that blocks access to a 32-bit-specific folder (such as Windows\system32), the rule does not work on 64-bit clients. You must also create a rule to block access to the Windows\syswow64 folder as well.

**Table 471: Application Control Rule options**

Group or Option	Description
Rule set name	The name of this collection of rules.
Description	A description of this collection of rules.
Enable logging	Clear this checkbox if you do not want information about this rule to be logged.
Enable this rule	Clear this checkbox if you do not want to immediately implement this rule.
Rules	Lists the rules in this collection of rules. You can have multiple rules in a collection of rules. The order of the rules is important; the rules that were created first have precedence. You can Add under the Rules list to add a new rule (application rule). Each rule may have multiple conditions. You can click Add under the Rules list to add a new condition to a rule. You can add the following conditions: <ul style="list-style-type: none"> <li>• <b>Registry Access Attempts</b></li> <li>• <b>File and Folder Access Attempts</b></li> <li>• <b>Launch Process Attempts</b></li> <li>• <b>Terminate Process Attempts</b></li> <li>• <b>Load DLL Attempts</b></li> </ul>

Group or Option	Description
<b>Properties</b>	<p>Configure the properties of the currently selected rule.</p> <p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Rule name</b></li> <li>• <b>Description</b></li> <li>• <b>Enable this rule</b></li> <li>• <b>Apply this rule to the following processes</b></li> <li>• <b>Do not apply this rule to the following processes</b></li> </ul> <p>By default, this rule is not applied to any process. This rule is applied to the processes listed under <b>Apply this rule to the following processes</b>. Processes listed under <b>Do not apply this rule to the following processes</b> are the exceptions to the processes that it is applied to. The list does not need to include all processes to which the rule does not apply.</p>
<b>Sub-processes inherit conditions</b>	Choose this option to allow child process definitions to inherit the conditions from the parent process.

## Registry Access Attempts properties

Use this tab to add a condition and to specify how this rule handles registries within that condition.

**Table 472: Registry Access Attempts properties options**

Group or option	Definition
Name	The name of this registry condition.
Description	A description of the registry condition.
Enable this condition	<p>Check or uncheck to enable or disable this condition in the rule set. Use this parameter to disable the conditions that you do not want to delete but do not want to apply yet.</p> <p>By default, this parameter is enabled.</p>
Apply to the following registry keys	You can add, edit, or delete registry keys from this list. Registry keys that are included in this list have the current condition applied to them when this policy is applied to a client.
Do not apply to the following registry keys	You can add, edit, or delete registry keys from this list. Registry keys that are included in this list do not have the current condition applied to them when this policy is applied to a client.

## Add Registry Key Definition

Use this dialog box to create the registry key definition for the condition.

**Table 473: Target registry key definition options**

Option	Description
<b>Registry key</b>	The registry key name. For example: HKEY_CLASSES_ROOT\*
<b>Registry value name</b>	Leave blank to match all value names.

Option	Description
<b>Registry value data</b>	<p>Leave blank to match any data.</p> <p><b>Note:</b> The data is treated as a string and not a number. For example, you might create a registry key condition with the name AAA and a registry key value of 111. If you configure the rule to block, then the rule only blocks AAA when it is created as a string.</p>
<b>Use wildcard matching</b>	By default, this option is enabled.
<b>Use regular expression matching</b>	<p>Check this option to use regular expression syntax to match the registry entries when this rule is used as part of the policy.</p> <p><a href="#">Regular expressions in custom IPS signature content and application control rules</a></p>

## Registry Access or File and Folder Access Attempts: Actions tab

You can set up read-access and write-access rights for registry access or file and folder access conditions in a rule.

### NOTE

If you create a custom rule that blocks access to a 32-bit-specific folder (such as Windows\system32), the rule does not work on 64-bit clients. You must also create a rule to block access to the Windows\syswow64 folder as well.

**Table 474: Action options**

Group or Option	Description
<b>Read Attempt</b>	<p>Select one of the following actions: <b>Continue processing other rules</b>, <b>Allow access</b>, <b>Block access</b>, or <b>Terminate process</b>. By default, <b>Continue processing other rules</b> is selected. If you select <b>Allow</b>, then this rule may conflict with another rule that blocks or terminates a process.</p> <p>Check <b>Enable logging</b> to log the action when this rule is applied. You can also select the severity level.</p> <p><b>Note:</b> If you enable logging, two log entries might appear in the Control log for a single event. For example, two entries might appear if an application reads and then tries to write a file.</p> <p><b>Note:</b></p> <p>You must check <b>Enable logging</b> and <b>Send Email Alert</b> if you set up administrator notifications for application control on the <b>Monitors</b> tab.</p> <p>Check <b>Notify user</b> if you want to notify the user when the defined action is taken. You can type the text that displays on the client computer. The operating system limits the amount of text that can be displayed in this notification on a client computer. To avoid the truncation of the notification text, you should limit your added text to no more than 120 characters.</p>
<b>Create, Delete, or Write Attempt</b>	<p>The same options are available.</p> <p><b>Note:</b> If you enable logging, the events that appear in the Control log might show a file size as 0 bytes rather than the actual file size. Typically, the file size appears as 0 bytes when the application control rule triggers before a process creates or writes a file.</p>

## File and Folder Access Attempts properties

This condition allows or blocks access to defined files or folders on client computers. When you apply a condition to everything in a given folder, use the wildcard, as in {folder name}\\*.

**Table 475: File and Folder Access Attempts properties options**

Option	Description
Name	The name of the condition.
Description	A description of the condition's function.
Enable this condition	Enables or disables this condition.
Apply to the following files and folders	You can add, edit, or delete files and folders from this list. The actions for this condition are applied to the files and folders in this list.
Do not apply to the following files and folders	You can add, edit, or delete files and folders from this list. The actions for this condition are not applied to the files and folders in this list.

## Launch or Terminate Process Attempts properties

Use this tab to specify information about how this rule handles applications attempting to launch processes or terminate processes.

**Launch Process Attempts** allows or blocks the ability to launch a process on a client computer

**Terminate Process Attempts** allows or blocks the ability to terminate a process on a client computer. For example, you may want to block a particular application from being stopped. This condition does not prevent an application from being terminated using normal methods of quitting an application, such as `Alt-F4`, or the program's native exit routine. It prevents the process from being terminated by other applications or procedures.

**Table 476: Launch or Terminate Process Attempts properties options**

Option	Definition
Enable this condition	The condition must be enabled to be applied. Uncheck to disable the condition if you are not ready to apply it yet.
Apply to the following processes	The condition applies to the processes that are included in this list. Click <b>Add</b> to type the process you want to block or kill. For example: <code>C:\Program Files\Mozilla Firefox\firefox.exe</code>
Do not apply to the following processes	The condition ignores the processes that are included in this list. This list includes exceptions to the processes that are listed under <b>Apply to the following processes</b> . It does not list every process to which this condition does not apply.

## Add Process Definition

Use this dialog box to add process definitions to the rule.

**Table 477: Add process definition options**

Group or Option	Description
<b>Process name to match</b>	<p>Type the process name to match with this rule. If you use this option, you cannot use the Match the file fingerprint option, which is available when you click Options.</p> <p>You can use environment variables, wildcards, and registry keys. Environment variables are useful when you have the clients that may be running various versions of Windows operating systems. For example, %windir%\calc.exe matches any path to the calc.exe application.</p> <p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Use wildcard matching (* and ?supported)</b></li> <li>• <b>Use regular expression matching</b>  <a href="#">Regular expressions in custom IPS signature content and application control rules</a></li> <li>• <b>Only match processes running from the following drive types</b>            You can check the drive types that you want to match on.  <b>Note:</b> You cannot block writing to DVD drives even if you select <b>DVD drive</b>.  <b>Note:</b> For the latest information, see the Symantec Knowledge Base document: <a href="#">After setting up an Application and Device Control policy to block DVD writing, DVD writing is not blocked as expected, and write attempt is not logged</a>.</li> <li>• <b>Only match processes running on the following device id type</b>            If you do not want to type a device ID type, you can click <b>Select</b> to select a device from the device list. The device list contains the device instance name and the device instance ID.  <b>Note:</b> An application may have more than one process. You might need to add multiple processes if you want to block or allow a particular application.</li> </ul>
<b>Match the file fingerprint</b>	<p>A file fingerprint is a checksum of an executable or DLL on a client computer. To ensure that the correct file is allowed or blocked, Symantec recommends that you calculate an MD5 hash or SHA256 hash (14.3 RU1 and later) of the file.</p> <p>When an update for a program is available and its executable modified, you need to create and add a new MD5 or SHA256 hash. Hashes are necessary for all versions of the executable that may be in use.</p> <p>Some MD5 hash tools may provide hash values of files in the C:\Windows\SysWOW64\ folder, even though you request values for files in the C:\Windows\System32\ folder. Symantec's checksum.exe tool (recommended) generates hash values for the exact file path requested.</p> <p>To get either the MD5 hash or SHA256 hash, run the checksum tool with the -csv flag. For example, type: <code>checksum.exe &lt;output file&gt; -csv</code> or <code>checksum.exe &lt;output file&gt; -csv &lt;directories to scan&gt;</code>. You can cut and paste the hash value in the output file into the Application Control rule.</p> <p><a href="#">Creating a file fingerprint list with checksum.exe</a></p>



Group or Option	Description
<b>Only match processes with the following arguments</b>	<p>This option is available when you select <b>Options</b>. Check this option if you want to include specific arguments in the available text box.</p> <p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Match exactly</b></li> <li>• <b>Use regular expression matching</b></li> </ul> <p><a href="#">Regular expressions in custom IPS signature content and application control rules</a></p>

## Launch Process, Terminate Process, or Load DLL Attempts: Actions tab

Use this tab to configure the action that you want to occur when a monitored process satisfies a condition of this rule.

**Table 478: Actions tab options**

Option	Description
<b>&lt;Condition name&gt; Attempt</b>	<p>Select the action that you want to occur when the monitored process meets this rule's condition.</p> <ul style="list-style-type: none"> <li>• <b>Continue processing other rules</b> Lets you log the event and continue processing other rules in the stack. The standard operation is to stop processing rules once the first criteria matches. This option is the default.</li> <li>• <b>Allow access</b> Allows the operation to continue.</li> <li>• <b>Block access</b> Prevents the operation.</li> <li>• <b>Terminate process</b> Kills the application making the request, or the caller process.</li> </ul> <p><b>Warning!</b> Make sure that you use the best action or else you might end up with undesirable results. For example, Symantec recommends that you use <b>Block access</b> rather than <b>Terminate process</b>, which can cause system instability or an unexpected restart. <b>Block access</b> blocks the target process that you defined for the condition. <b>Target process</b> kills the caller process, which you defined for the rule.</p> <p>For <b>File and Folder Access Attempts</b> and <b>Registry Access Attempts</b>, you can configure one action for read attempts. You can configure a different action to be taken for create, delete, and write attempts. If you allow this process, then this rule may conflict with another rule that blocks or terminates a process.</p>
<b>Enable logging</b>	<p>Logs the action in the Application Control log when the rule condition is applied.</p> <p>You must check <b>Enable logging</b> and <b>Send Email Alert</b> if you set up administrator notifications for application control on the <b>Monitors</b> tab.</p> <p>If you enable logging, two log entries might appear in the Control log for a single event. For example, two entries might appear if an application reads and then tries to write a file. Two entries also appear if an application writes and then tries to delete a file.</p>
<b>Notify user</b>	<p>Displays a message on the client computer when this rule is applied.</p> <p>The operating system limits the amount of text that can be displayed in this notification on a client computer to 255 characters. The amount of custom text that displays may vary, and depends on the length of the rule name and the file name. To avoid the truncation of the notification text, you should limit your added text to no more than 120 characters. This recommendation does not guarantee the display of all custom text.</p>

---

## Load DLL Attempts properties

Use this tab to specify information about how this rule handles DLLs.

**Table 479: Load DLL Attempts properties options**

Option	Description
Name	The name of this rule condition.
Description	A description of this rule condition.
Enable this condition	Check or uncheck to enable or disable this condition in the Application and Device Control Policy. Use this parameter to disable a condition that you do not want to delete but do not want to apply yet. By default, this option is enabled.
Apply to the following DLLs	You can add, edit, or delete DLLs from this list. DLLs included in this list will have the current condition applied to them when this policy is applied to a client.
Do not apply to the following DLLs	You can add, edit, or delete DLLs from this list. DLLs included in this list will not have the current condition applied to them when this policy is applied to a client.

## Add DLL Definition

Use this tab to define options for the DLL that you want to match with this condition.

**Table 480: DLL definition options**

Option	Description
<b>DLL name to match</b>	<p>Type the DLL name to match with this condition. You can use environment variables, wildcards, and registry keys. If you use this option, you cannot use the Match the file fingerprint option, which is available when you select <b>Options</b>.</p> <p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>Use wildcard matching (* and ? supported)</b></li> <li>• <b>Use regular expression matching</b>  <a href="#">Regular expressions in custom IPS signature content and application control rules</a></li> <li>• <b>Only match DLLs loading from the following drive types</b></li> <li>• <b>Only match processes running on the following device id type</b>            If you do not want to type a device ID type, you can click <b>Select</b> to select a device from the device list. The device list contains the device instance name and the device instance ID.</li> </ul>
<b>Match the file fingerprint</b>	<p>A file fingerprint is a checksum of an executable or DLL on a client computer. To ensure that the correct file is allowed or blocked, Symantec recommends that you calculate an MD5 hash or SHA256 hash (14.3 RU1 and later) of the file.</p> <p>When an update for a program is available and its executable modified, you need to create and add a new MD5 or SHA256 hash. Hashes are necessary for all versions of the executable that may be in use.</p> <p>Some MD5 hash tools may provide hash values of files in the C:\Windows\SysWOW64\ folder, even though you request values for files in the C:\Windows\System32\ folder. Symantec's checksum.exe tool (recommended) generates hash values for the exact file path requested.</p> <p>To get either the MD5 hash or SHA256 hash, run the checksum tool with the -csv flag. For example, type: <code>checksum.exe &lt;output file&gt; -csv</code> or <code>checksum.exe &lt;output file&gt; -csv &lt;directories to scan&gt;</code>. You can cut and paste the hash value in the output file into the Application Control rule.</p> <p><a href="#">Creating a file fingerprint list with checksum.exe</a></p>

## Device Control

For each type of policy, you can create a hardware device control list. This list contains a list of blocked devices and a list of devices that are excluded from blocking.

The list does not show all of the allowed devices. This list only displays the exceptions to the **Blocked Devices** list.

### NOTE

Symantec recommends that you do NOT select ports or network adapters as devices to be blocked. If you select those devices, clients with this policy applied lose all network connectivity.

**Table 481: Device blocking options**

Group or option	Description
Device Name	The name of the device that is blocked or excluded from blocking. You can add or delete devices from this list.
Identification	The identifier of the device that is blocked or excluded from blocking. The identifier can be either the class ID or the device ID.
Log detected devices	Adds an entry to the security log whenever Device Control blocks a device, or when a device is detected that is excluded from blocking. This option is enabled by default.
Notify users when devices are blocked or unblocked	Sends a notification to client computers when a blocked device is connected or starts up. This option is disabled by default. Use the <b>Specify Message Text</b> option to create a custom message that appears in the notification. The operating system of the client computer limits the amount of text that can appear in the notification. To avoid the truncation of the notification text, you should use no more than 120 characters in the message.

## Mac Device Control in Endpoint Protection 14

For each type of policy, you can create a hardware device control list. This list contains a list of blocked devices and a list of devices that are excluded from blocking.

The hardware device control occurs at the file system level. Therefore, the user may still be able to perform volume-level tasks on blocked devices or read-only devices with Disk Utility or Terminal commands. These tasks include erasing, ejecting, or creating a disc image of the blocked device.

The list does not show all of the allowed devices. This list only displays the exceptions to the **Blocked Devices** list.

You should test all device control conditions that you create on a small test group before you apply the policy to all Mac clients. Testing ensures the device control policy blocks devices and excludes devices from blocking as expected.

### NOTE

Use caution when blocking by vendor or device ID. Symantec recommends that you do not select non-storage devices that may show up in Finder as devices to be blocked.

You can configure client user interface control settings with **Server Control** or **Mixed Control** mode to prevent users from enabling or disabling device control.

[Preventing users from disabling protection on client computers](#)

[Mac device blocking options](#) lists the device blocking options available for Mac devices.

[Regular expressions used for device blocking for Mac](#) describes the regular expressions with which you can define device control criteria.

Vendor, model, and serial number fields are not case-sensitive. For each device specified, if you leave the vendor, model, or serial number fields blank, the policy blocks any devices that match the device type.

Device control rule conditions give greater precedence to the criteria that are the most specific. For example, the full text string has the greatest precedence, followed next by a partial text string with wildcard, and then by a wildcard only. A blank field acts like a wildcard search, with less weight than the full text string or a partial text string. Similarly, the serial number has a greater precedence than the model name, which takes greater precedence than the vendor name. The full string text for the vendor name takes precedence over the partial string text of the serial number.

The Mac device control conditions are weighted as follows, from greatest weight to least:

- Full string text, serial number
- Full string text, model name
- Full string text, vendor name
- Partial string text with wildcard, serial number
- Partial string text with wildcard, model name
- Partial string text with wildcard, vendor name
- Wildcard only, serial number
- Wildcard only, model name
- Wildcard only, vendor name
- Blank field (nothing defined)

To obtain the serial number, model number, or vendor name from a Mac-connected device, use the DeviceInfo tool from the installation file. You can find this tool and its instructions under `Tools/DeviceInfo`.

**Table 482: Mac device blocking options**

Group or option	Description
Device Name	<p>The name of the device that is blocked or excluded from blocking. You can add or delete devices from this list.</p> <p>The supported device types for Mac are:</p> <ul style="list-style-type: none"> <li>• Thunderbolt devices</li> <li>• CD/DVD drives</li> <li>• USB devices</li> <li>• FireWire devices</li> <li>• Secure digital (SD) card</li> </ul>
Device Vendor	<p>The vendor of the device that is blocked or excluded from blocking.</p> <p>You can block or exclude from blocking all device types except Thunderbolt by specific vendor name.</p> <p>You can use regular expressions to define the vendor name.</p> <p><a href="#">Regular expressions used for device blocking for Mac</a></p>
Device Model	<p>The model of the device that is blocked or excluded from blocking. You can block or exclude from blocking all device types by specific model.</p> <p>You can use regular expressions to define the model name.</p> <p><a href="#">Regular expressions used for device blocking for Mac</a></p>
Serial Number	<p>The serial number of the device that is blocked or excluded from blocking.</p> <p>You can only block or exclude from blocking the specific serial numbers of Thunderbolt and USB devices.</p> <p>You can use regular expressions to define the serial number.</p> <p><a href="#">Regular expressions used for device blocking for Mac</a></p>
Log detected devices	<p>Adds an entry to the device control log whenever Device Control detects a device. This option is enabled by default.</p>
Notify users when devices are blocked or unblocked	<p>Sends a notification to client computers when a blocked device connects or starts up. This option is disabled by default.</p>

**Table 483: Regular expressions used for device blocking for Mac**

Option	Description
. (Dot)	Matches any character but a newline. For example, <code>So*.*</code> matches "So", "Soo", "Sooo", "Sobar", "Sooxxx".
\ (Backslash)	Matches the character to follow. The backslash escapes all other meta-characters and itself. When you use backslash in a set, it is considered a regular character. For a binary match, use <code>\x</code> . For example, <code>\xA0</code> matches binary a0 Hex.
[set], [^Set] (Set)	Matches one of the characters in the set. If the first character in the set is a caret ( <code>^</code> ), the set attempts to match any characters that are not in the set. The special characters right bracket ( <code>]</code> ) and hyphen ( <code>-</code> ) have no special meaning if they appear as the first character in the set. A set can also match a range or characters. For example, <code>S-E</code> would specify a set of characters S through E, inclusive. For example, <code>[a-z]</code> matches any alphabetical character, while <code>[^]-]</code> matches any character except for <code>]</code> , <code>\</code> , and <code>-</code> .
* (Star or asterisk)	Any previous regular expression form that concludes with the asterisk ( <code>*</code> ) matches zero or more matches of that form. For example, <code>Soo\*</code> matches "Soo", "Soo\\", "Soo\\", and "Soo\\12".
+ (Plus)	Any previous regular expression form that concludes with the plus ( <code>+</code> ) matches one or more matches of that form. For example, <code>Soo\+</code> matches "Soo", "Soo\\", and "Soo\\", but it does not match "Soo\\12".

## Add Notification Message

Use this dialog box to type the text that appears in notification messages sent to users that attempt to access devices in the Blocked Devices list.

## Hardware Device

Use this dialog box to add devices to or edit devices in the **Hardware Devices** list. You can use the **Hardware Devices** list when you configure device control.

You cannot add or edit customized devices for Mac.

**Table 484: Hardware device options**

Field	Description
Device Name	Type a descriptive name for the device or category of devices.
Class ID	Type the class ID of the device. You can use the Registry Editor or the <code>DevViewer</code> utility to find the class ID of the hardware device.
Device ID	Type the device ID provided by the manufacturer. You can use Device Manager control panel or the <code>DevViewer</code> utility to find the device ID of a hardware device.

[Obtaining a device vendor or model for Windows computers with DevViewer](#)

# Firewall Policy

## Rules: Rules

Use this tab to work with firewall rules. You can add, edit, delete, copy, paste, import, export, inherit, enable or disable, and change the order of firewall rules.

Table 485: Rules tab

Option	Description
Inherit Firewall Rules from Parent Group	Inherits only the rules from a parent group's Firewall policy. You cannot inherit rules from a policy in a location that inherits all its policies from a parent group. <a href="#">Adding inherited firewall rules from a parent group</a>
Firewall Rules	Displays the firewall rules. You can add, edit, delete, and move rules in this list. The list contains a blue dividing line. Rules that appear above the dividing line are of higher priority than those that appear under the line. You can use the line to separate the rules that are inherited from a parent group and those that have been implemented at the subgroup level. The dividing line also lets you set up the priority of rules for clients in mixed control. Rules above the line take precedence over the rules that the user creates on the client. The rules and the security settings that the users apply to their clients are merged with the rules that the console deploys to the client.
Add Rule	Adds a rule by using a wizard that lets you configure the action, hosts, network services, and logging settings for the rule.
Add Blank Rule	Adds a blank rule to the <b>Rules</b> list. The firewall ignores the settings in a blank rule.
Move Up or Move Down	Moves the rule up one row or down one row. Rules are processed in the order that they appear in the table.

The Rules list displays the default firewall rules, the inherited rules, and the rules that you create. The firewall rules are listed and enforced in the order that they are numbered.

Table 486: Rules list columns

Column name	Description
No	Displays the order that the firewall processes the rules. You can reorder rules to change priorities.
Enabled	Enables the rule. If unchecked, the firewall ignores the rule.
Name	Displays the name of the rule. Click the name to edit it.
Action	<b>Specifies what happens to traffic if the traffic matches the following rule conditions:</b> <ul style="list-style-type: none"><li>• <b>Allow</b> Allows any communication of this type to take place.</li><li>• <b>Block</b> Prevents any communication of this type.</li><li>• <b>Ask</b> Asks the user to either allow the traffic or block the traffic.</li></ul> Double-click the action to change it.

Column name	Description
<b>Application</b>	<p>Specifies the applications that trigger the rule.</p> <p><b>If the application is detected, the rule takes effect. You can specify an application in the following ways:</b></p> <ul style="list-style-type: none"> <li>• Define an application by file name, description, size, last modified, and file fingerprint.</li> <li>• Select from a list of applications that your client computers run.</li> </ul> <p><a href="#">Application List</a></p>
<b>Host</b>	<p>Specifies the hosts that trigger the rule.</p> <p>You can identify the specific DNS domain, DNS host, IP address, IP address range, MAC address, or subnet for the computers.</p> <p><a href="#">Add or Edit Host</a></p>
<b>Service</b>	<p>Specifies the services that trigger the rule.</p> <p>Typically, specific types of services occur on specific ports. For example, Web traffic (HTTP and HTTPS) generally occurs on ports 80 and 443. The Service list lets you group multiple ports together.</p> <p>You can select a service from the list, or you can define additional services.</p> <p>You can apply the rule to inbound network traffic, outbound network traffic, or network traffic in both directions.</p> <p><a href="#">Protocol</a></p>
<b>Log</b>	<p>Specifies whether the server creates a log entry or sends an email message when a traffic event matches the criteria that are set for this rule.</p> <p><b>You can select one or more of the following log options:</b></p> <ul style="list-style-type: none"> <li>• <b>Write to Traffic Log</b></li> <li>• <b>Write to Packet Log</b></li> <li>• <b>Send Email Alert</b></li> </ul> <p>To send email messages, you must configure a client security alert to appear for any firewall activity on the <b>Notifications</b> tab of the <b>Monitors</b> page.</p> <p><a href="#">Add or Edit Notification Condition</a></p>
<b>Severity</b>	<p>Assigns a level of importance to the event.</p> <p>The Security Log displays the severity.</p>
<b>Adapter</b>	<p>Specifies the adapters that trigger the rule. You can select one or more of the following adapters:</p> <ul style="list-style-type: none"> <li>• <b>All Adapters</b></li> <li>• <b>Any VPN</b></li> <li>• <b>Dial-up</b></li> <li>• <b>Ethernet</b></li> <li>• <b>Wireless</b></li> <li>• <b>More Adapters</b></li> </ul> <p>Enables you to choose from a list of vendor-specific adapters or custom adapters that you add.</p> <p>Adapter-based rules are available only for Windows.</p>
<b>Time</b>	<p>Time period during which the rule is active or inactive. You can set up a schedule to include or exclude a time period during which the rule is active. You must enter time in UTC format.</p>
<b>Screen Saver</b>	<p>Specifies which of the following states of the screen saver affects the rule:</p> <ul style="list-style-type: none"> <li>• <b>On</b></li> <li>• <b>Off</b></li> <li>• <b>Any</b></li> </ul> <p>The state of the screen saver does not affect the rule.</p>
<b>Created At</b>	<p>Specifies whether the policy was created as a shared policy or a non-shared policy for an individual location. A group name, such as Sales, appears for a non-shared policy.</p> <p>This column is informational only.</p>
<b>Description</b>	<p>Provides the additional information for the rule, such as how it works.</p> <p>Use a description to distinguish the difference between similar rules.</p>

[Adding a new firewall rule](#)



---

## Application List

Use the Application List to define an application that triggers the rule. You can define an application by entering specific details about the application or by searching from a list of learned applications. Learned applications are a list of applications that the clients run.

## Add Application

Use this dialog box to define an application that triggers this firewall rule.

### NOTE

Network Application Monitoring must be enabled to define a firewall rule by all fields except for **Field Name**. If Network Application Monitoring is disabled, rule processing ignores the content in those fields.

[Blocking networked applications that might be under attack](#)

**Table 487: Application options**

Option	Description
<b>File Name</b>	The path name and file name of the application you want to add to the applications list for this rule. For example, you can type either <code>c:\program files\internet explorer\iexplore.exe</code> or <code>iexplore.*</code> . You can use wildcard character, including <code>*</code> or <code>?</code> . The path name is on the client.
<b>File Description</b>	The description of the application, such as Internet Explorer.
<b>Size</b>	The exact size of the application, in bytes, such as 2534879.
<b>Last Modified</b>	The date that the application was last saved, displayed in the following format: <ul style="list-style-type: none"><li>• <b>Year</b></li><li>• <b>Month</b></li><li>• <b>Day</b></li></ul>
<b>File Fingerprint</b>	<p>The file fingerprint is a checksum that uniquely identifies a file and is more unique than a file name. The fingerprint is a 128-bit or 256-bit string that you create with an MD5 hashing algorithm or an SHA-256 hashing algorithm. For example, <code>Cfca3291df528430fb6b2c526e9a04d0</code>.</p> <p>To create a file fingerprint, you can use the <code>checksum.exe</code> tool that is installed with the client. The tool creates an MD5 file fingerprint for the applications that runs on a particular client. You can also use the third-party tools that use MD5 or SHA-256 to create file fingerprints.</p> <p>The application learning feature in the console computes both the MD5 and the SHA-256 checksum for the applications that it learns. You can use the <b>Search for applications</b> option on the <b>Policies</b> page to get file fingerprint details for applications. Application learning must be enabled in the client communications settings.</p> <p>File fingerprints are useful if you want to add an application that has more than one version. You add a separate application with the unique file fingerprint for each version. For example, you would add both Internet Explorer 10 and Internet Explorer 11 with their respective file fingerprints as separate applications in the firewall rule.</p>

## Network Adapter

Use this dialog box to specify a network adapter that triggers a firewall rule. If you enable an adapter from the list, the firewall rule ignores all other adapters.

You can add, edit, and delete a custom network adapter to the list of adapters that are installed by default, for the specified rule only. The network adapters that you add in this dialog box are not available for other Firewall policies. To add a network adapter that is accessible by all Firewall policies, you must add them through the **Policy Components** list.

**Table 488: Network adapter options**

Option	Description
Apply the rule to all adapters	Applies the rule to any adapter, not just the adapters that are listed.
Apply the rule to the following adapters	Applies the rule only to the adapters that are enabled. You can select this option to add, edit, or remove a custom network adapter for the selected rule. You cannot edit or remove a default network adapter.
Adapter list	Lists the adapters you can enable. The list displays the description and the manufacturer's name of each adapter.

## Windows Integration

Use this dialog box to control when Windows Firewall is enabled and whether or not it displays an enabled message on client computers.

[Disabling the Windows Firewall](#)

**Table 489: Windows Integration Options**

Option	Description
<b>Disable Windows Firewall</b>	<p>Configures the action that Symantec Endpoint Protection takes when it detects Windows Firewall on the client computer. Windows Firewall is restored to the state it was in before Symantec Endpoint Protection installation if you:</p> <ul style="list-style-type: none"> <li>• Uninstall Symantec Endpoint Protection.</li> <li>• Disable the Symantec Endpoint Protection firewall.</li> </ul> <p>Symantec Endpoint Protection retains the Windows Firewall setting when you do a fresh installation of the product.</p> <p><b>The following options are available:</b></p> <ul style="list-style-type: none"> <li>• <b>No Action</b> Does not change the current Windows Firewall setting.</li> <li>• <b>Disable Once Only</b> Disables Windows Firewall at startup the first time Symantec Endpoint Protection detects that Windows Firewall is enabled. On subsequent startups, Symantec Endpoint Protection does not disable Windows Firewall.</li> <li>• <b>Disable Always</b> Disables Windows Firewall at every startup if Symantec Endpoint Protection detects that Windows Firewall is enabled.</li> <li>• <b>Restore If Disabled</b> Enables Windows Firewall at startup.</li> </ul> <p><b>Note:</b> For Windows 7 and later, Symantec Endpoint Protection takes control of Windows Firewall instead of disabling it. The Windows Firewall control panel displays the message <b>These settings are being managed by vendor application Symantec Endpoint Protection</b>. However, the options available in this policy still function as expected.</p>
<b>Windows Firewall Disabled Message</b>	<p>Configures Windows Firewall status message that displays on client computers when they boot up.</p> <ul style="list-style-type: none"> <li>• <b>Enable</b> Displays a startup message on client computers indicating that Windows Firewall is disabled.</li> <li>• <b>Disable</b> Suppresses the display of a message at startup indicating that Windows Firewall is disabled.</li> </ul>

## Network Adapter

You can add a new network adapter to the default list of network adapters. You can then enable the network adapter to allow or block in a firewall rule.

---

## NOTE

The client does not filter or detect network traffic from Personal Digital Assistant (PDA) devices.

**Table 490: Custom adapter options**

Option	Description
<b>Adapter Type</b>	The type of adapter. Adapters are hardware. They allow each computer in the network communicate with other computers.
<b>Adapter Name</b>	A description of the adapter. <b>Note:</b> This option is only available if you access this dialog box from the Policy Components list.
<b>Adapter Identification</b>	The manufacturer and the brand name of the adapter. To find the name of the adapter, you can open a command line on the client computer, and then type <code>ipconfig/all</code> .

## Select Host

Use this page to define which devices trigger the firewall rule.

By default, any host triggers the firewall rule. You can also add a specific host, or a host group to trigger the firewall rule. To add a host that is accessible to any Firewall policy, create a host group with multiple hosts in **Policy Components**. The host group then appears automatically in the Host List.

All hosts are enabled by default.

You can specify an address or a host name for the following situations:

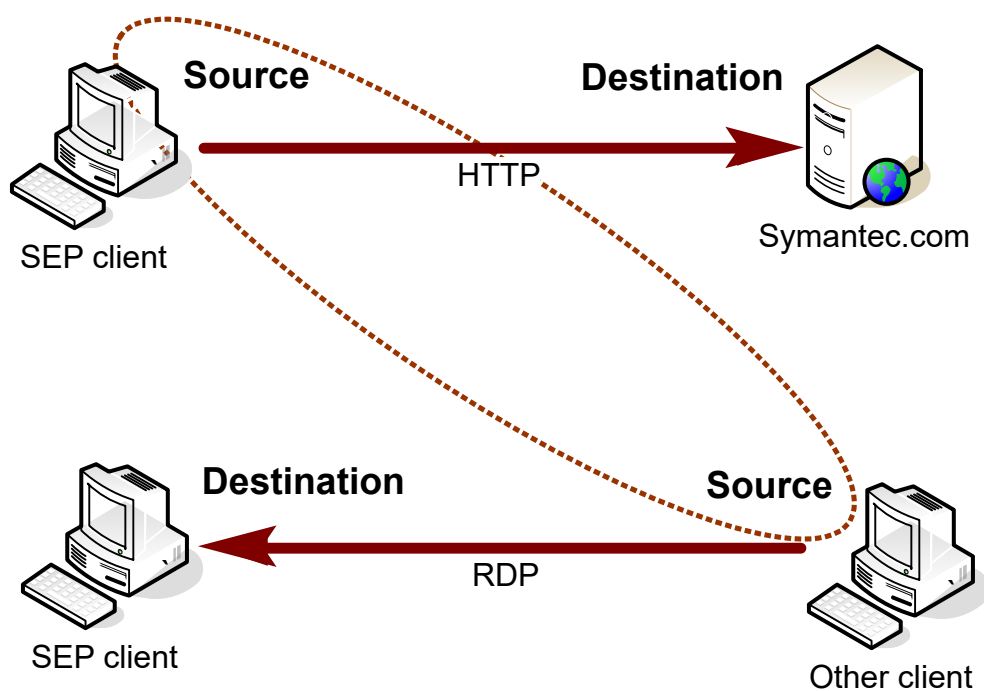
- A device that the client excludes from checks by the firewall or IPS signatures.
- A device that the authenticator client excludes from the peer-to-peer authentication process. The authenticator normally blocks traffic from a remote client that tries to connect to the authenticator. The authenticator does not block computers in this list. For peer-to-peer authentication, you can only specify the IP address, IP range, and subnet. Some address types are supported for defining hosts in Firewall policies but not for Intrusion Prevention policies.

You define the host either by the source and the destination host relationship, or the remote and the local host relationship. Either method provides the same functionality. You can define multiple source hosts and multiple destination hosts.

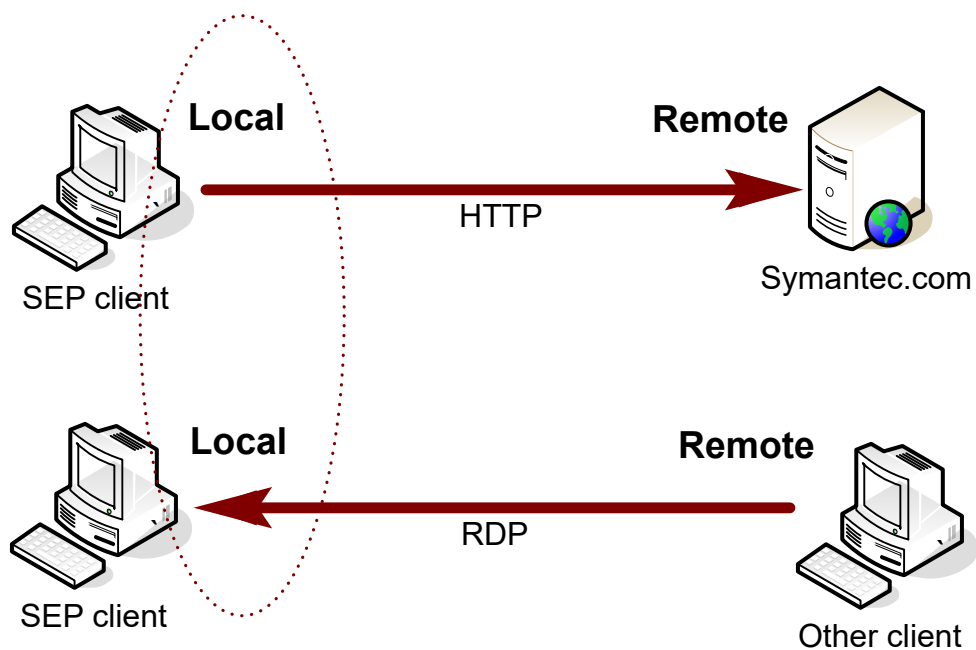
**Table 491: Source/destination hosts and local/remote hosts**

Option	Description
<b>Source/Destination</b>	The source host and destination host are dependent on the direction of traffic. In one case the local client computer might be the source, whereas in another case the remote computer might be the source. This relationship are more commonly used in network-based firewalls.
<b>Local/Remote</b>	The local host is always the local client computer, and the remote host is always a remote computer that is positioned elsewhere on the network. This expression of the host relationship is independent of the direction of traffic. This relationship is more commonly used in host-based firewalls, and is a simpler way to look at traffic.

[The relationship between source and destination hosts](#) illustrates the source relationship and destination relationship with respect to the direction of traffic.



The relationship between local and remote hosts illustrates the local host and remote host relationship with respect to the direction of traffic.



Relationships are evaluated by the following types of statements:

The hosts that you define on either side of the connection (between the source and the destination)	OR statement
Selected hosts	AND statement

For example, consider a rule that defines a single local host and multiple remote hosts. As the firewall examines the packets, the local host must match the relevant IP address. However, the opposing sides of the address may be matched to any remote host. For example, you can define a rule to allow HTTP communication between the local host and either Symantec.com, Yahoo.com, or Google.com. The single rule is the same as three rules.

## Add or Edit Host

You can specify an address or a host name for the following computers:

- A computer that triggers a firewall rule
- A computer that the client excludes from checks by the firewall or IPS signatures.
- A computer that the authenticator client computer excludes from the peer-to-peer authentication process. The authenticator normally blocks traffic from a remote client that tries to connect to the authenticator. The authenticator does not block computers in this list. For peer-to-peer authentication, you can only specify the IP address, IP range, and subnet.

### NOTE

Some address types are supported for defining hosts in Firewall policies but not for Intrusion Prevention policies.

**Table 492: Host configuration options**

Type	Description
<b>Address Type</b>	<p>The address type of the host for which connections are allowed or blocked.</p> <p><b>You choose one of the following options to define a host:</b></p> <ul style="list-style-type: none"> <li>• <b>DNS domain</b> (Firewall only) A unique address that devices use to communicate with each other using the DNS domain.</li> <li>• <b>DNS host</b> (Firewall only) A unique address that devices use to communicate with each other using the DNS host.</li> <li>• <b>IP address</b> A unique address that devices use to communicate with each other using the IP address. For firewall policies, you can specify IPv4 or IPv6. <b>IP address</b> is the default address type.</li> <li>• <b>IP range</b> <b>Start</b> IP address and <b>End</b> IP address that identifies a block of IP addresses. For firewall policies, you can specify IPv4 or IPv6.</li> <li>• <b>Local Subnet</b> (Firewall only) Allows traffic to the local subnet even if the IP address of the local subnet changes. This option only appears when you add or edit a host list directly in a Firewall policy.</li> <li>• <b>MAC address</b> (Firewall only) A unique address that devices use to communicate with each other using the MAC address.</li> <li>• <b>Subnet</b> A subnet lets you divide the host part of an IP address into two or more subnets. It identifies the network and the node parts of the address. For firewall policies, you can specify an IPv4 or IPv6 subnet mask. You specify <b>Subnet Address</b> and <b>Subnet Mask</b> for IPv4. The subnet mask format for IPv4 is nnn.nnn.nnn.nnn, such as 255.255.255.0. For IPv6, you enter the address and mask together in the <b>IPv6 Subnet Mask</b> text box.</li> </ul>

[Adding host groups](#)

---

## Host Groups

Use this dialog box to create a list of hosts. You can specify either a host name or an IP address of a computer that triggers a firewall rule. You can add multiple hosts to a host group, which is then accessible from any rule in the **Rules** list. If you add a host from the **Rules** list, it is only available from a single rule.

**Table 493: Host groups options**

Option	Description
<b>Group Name</b>	Specifies a name for a group of defined hosts
<b>Type</b>	Defines the host by DNS domain, DNS host, IP address, IP range, MAC address, or subnet.
<b>Content</b>	Defines the criteria for the host type.

## Schedule List

A rule is active or inactive during a specified time period. Use this dialog box to add, modify, or remove time periods.

All the time periods in the list are automatically enabled. If you want to disable a time period for the selected rule, you need to delete the entry from the table.

**Table 494: Schedule list options**

Option	Description
<b>Any Time Except</b>	Specifies the time period that the rule is not active. You must enter time in UTC format. You can uncheck the Any Time Except check box to apply the rule to the specified time period.
<b>Time</b>	Lists the start and the end time and frequency of the schedule. You must enter time in UTC format.

## Add Schedule

Use this dialog box to set up or edit a schedule during which a firewall rule is active or not active. For example, you may want the rule to be inactive during a time when you install new applications.

**Table 495: Scheduling options**

Option	Description
<b>Time Period</b>	<p>Specifies the time period that the firewall rule is active or inactive.</p> <p>The time period is based on the hour, minutes, and seconds when the time period starts and when it ends.</p> <p>For example, you might want the firewall to detect whether clients run certain applications during office hours. You would set the Start Time to 8 Hr and set the End Time to 17 Hr and 30 Min. You must enter time in UTC format.</p>
<b>Months &amp; Days</b>	<p><b>Specifies the frequency of the schedule, by using the following options:</b></p> <ul style="list-style-type: none"><li>• <b>Month</b> One month or all 12 months of the year.</li><li>• <b>Every day</b> All seven days of the week.</li><li>• <b>Weekends</b> Saturdays and Sundays only.</li><li>• <b>Weekdays</b> Monday through Friday.</li><li>• <b>Specify days</b> One or more days of the week.</li></ul> <p><b>Note:</b> If you consider the weekend to be something other than Saturday and Sunday, click <b>Specify days</b>.</p>

## Service List

A network service is a collection of protocols and port numbers that are grouped under one name. For example, the traffic that goes through an HTTP server uses TCP local ports 80 and 443. The network services list includes the most commonly used network services, such as a DHCP server and various VPNs.

You can add a network service for the selected rule only. If you create another rule, the service does not appear in the **Service List** for that rule. If you want to make the service available for any firewall rule, add the service to the **Network Service** list under **Policy Components**.

Any network services that you add from the firewall rules list are added to the top of the **Service List** for that rule. The network services that you add under **Policy Components** are added to the bottom of the **Network Service** list.

**Table 496: Network service options**

Option	Description
<b>Enable</b>	Activates the service. If unchecked, the rule ignores the service.
<b>Service Name</b>	<p>Lists the name of the service.</p> <p>You can add only one protocol per service.</p>
<b>Content</b>	Lists the protocol type for each service, and the port and the traffic direction that defines the protocol.

## Protocol

You can select which network services that you want to trigger the firewall rule. You can define the service based on its protocol, port, and the traffic direction.

---

You can define the following protocols:

<b>TCP</b>	Port or port ranges.
<b>UDP</b>	Port or port ranges.
<b>ICMP</b>	Type and code.
<b>IP</b>	Protocol number (IP type). Examples: Type 1 = ICMP, Type 6 = TCP, Type 17 = UDP This is the default when adding protocols.
<b>Ethernet</b>	Ethernet frame type. Examples: Type 0x0800 = IPv4, Type = 0x8BDD = IPv6, Type 0x8137 = IPX

[TCP and UDP protocol settings](#)

[ICMP, IP, and Ethernet protocol options](#)

When you define TCP-based or UDP-based service triggers, you identify the ports on both sides of the described network connection. Traditionally, ports are referred to as being either the source or the destination of a network connection.

You can define the network service relationship in either one of the following ways:

<b>Source/Destination</b>	The source port and destination port are dependent on the direction of traffic. In one case the local client computer might own the source port, whereas in another case the remote computer might own the source port.
<b>Local/Remote</b>	The local host computer always owns the local port, and the remote computer always owns the remote port. This expression of the port relationship is independent of the direction of traffic.

You specify the direction of traffic when you define the protocol.

You can define multiple protocols. For example, a rule might include the ICMP, IP and TCP protocols. The rule describes multiple types of connections that may occur between the identified client computers, or used by an application. When you add multiple TCP/UDP ports or protocol types, make sure you put a comma between them.



**Table 497: TCP and UDP protocol settings**

Option	Description
<b>Source/Destination</b>	<p>Specifies the port number in the following fields:</p> <ul style="list-style-type: none"> <li>• <b>Source Port</b> Port where the packet comes from. For inbound traffic, the source is the remote port. For outbound traffic, the source is the local port.</li> <li>• <b>Destination Port</b> Port where the packet is going to. For inbound traffic, the destination is the local port. For outbound traffic, the destination is the remote port.</li> </ul> <p>Click &gt;&gt; to view the available port numbers.</p> <p>For example, when the client computer connects to a remote desktop, the traffic is outbound, the source port is random, and the destination port is TCP 3389. If another computer connects to the client as a remote desktop, then the traffic is inbound but the source ports and destination ports stay the same. The source port is still random and the destination is 3389 on TCP.</p>
<b>Local/Remote</b>	<p>Sets the port number for the following fields:</p> <ul style="list-style-type: none"> <li>• <b>Local Port</b> Client computer</li> <li>• <b>Remote Port</b> Computer that communicates with the client computer</li> </ul> <p>Click &gt;&gt; to view the available port numbers.</p> <p>For example, when the client computer connects to a remote desktop, the remote port is TCP 3389. The local port is the same, for both inbound and outbound traffic.</p> <p>If you do not select a port number, then all the ports trigger the rule. If you enter a port number for the local port, but not for the remote port, then the local port that you entered and all the remote ports trigger the rule.</p>
<b>Direction</b>	<p>Specifies the following ways to specify traffic direction:</p> <ul style="list-style-type: none"> <li>• <b>Both</b> Traffic goes in both directions between the client and the network. This is the default.</li> <li>• <b>Incoming</b> Traffic goes from the network to the client.</li> <li>• <b>Outgoing</b> Traffic goes from the client to the network.</li> </ul>
<b>Stateful UDP</b>	<p>Maintains the stateful inspection of UDP sessions. TCP automatically includes stateful inspection.</p>

**Table 498: ICMP, IP, and Ethernet protocol options**

Protocol type	Description
<b>ICMP or ICMPv6</b>	<p>Controls the messages that report the errors in traffic communication, such as Echo Reply. The ICMP protocol includes the following fields:</p> <ul style="list-style-type: none"> <li>• <b>ICMP Type</b> Lists the protocols' ISO numeric designators. Click &gt;&gt; to view the list of available types and codes</li> <li>• <b>ICMP Code</b> The code fields for the ICMP type.</li> <li>• <b>Packet Direction</b> This default is <b>Both</b>.</li> </ul>
<b>IP</b>	<p>Specifies the following fields for the IP protocol:</p> <ul style="list-style-type: none"> <li>• <b>Protocol Type</b> The IP protocol numbers used in the protocol field of IPv4 packets and the header field of IPv6 packets. The &gt;&gt; to the right of the text box displays the list of available types and ISO numeric designators.</li> <li>• <b>Protocol Direction</b> The direction of the traffic between the network and the client. Traffic from the network to the client is inbound and traffic from the client to the network is outbound. This default is <b>Both</b>.</li> <li>• <b>Apply to fragmented packets only</b> The IP packets can be broken into smaller packets for network segments that can only handle smaller packets. To keep the firewall from blocking the incomplete packets, you can enable this option to allow the incomplete packets by using the ICMP protocol.</li> </ul>
<b>Ethernet</b>	<p>Specifies the following fields for the Ethernet protocol:</p> <ul style="list-style-type: none"> <li>• <b>Protocol Type</b> Ethertypes.</li> <li>• <b>Protocol Direction</b> Direction of the connection between the network and the client. This default is <b>Both</b>.</li> </ul> <p>Ethernet protocols are the group of LANs that are covered by the IEEE 802.3.</p>

## Network Service

A network service is a collection of protocols and port numbers that are grouped under one name. The network services list includes the most commonly used network services, such as a DHCP server and various VPNs. You can also add custom network services. You then choose either a predefined network service or a custom service to include in a firewall rule.

The network services that you define are added to the bottom of the list.

---

**Table 499: Network service options**

Option	Description
<b>Service Name</b>	The name of the service. If you add a service that is closely related to another service, you must type a description that denotes the difference.
<b>Protocol Type</b>	The protocol type for each service. You can list multiple protocols for each service. If you select a protocol, you can edit or delete it.
<b>Content</b>	The port number and traffic direction that defines the protocol.

## Built-in Rules

As of version 14.2, IPv4 and IPv6 are supported for references to IP. For earlier versions, only IPv4 is supported.

**Table 500: Allowed traffic protocols and other settings**

Option	Description
<b>Enable Smart DHCP*</b>	Allows only the outbound DHCP requests and inbound DHCP replies. Smart DHCP also allows DHCP renew. If you disable this setting, to use DHCP you must create a firewall rule that allows UDP traffic on remote ports 67 (bootps) and 68 (bootpc). The Dynamic Host Configuration Protocol (DHCP) is a protocol that assigns a dynamic IP address to a computer on a network. Dynamic addresses enable a computer to have a different IP address every time it connects to a corporate network. DHCP supports both the static IP addresses and the dynamic IP addresses. Dynamic addresses simplify network administration because the software keeps track of IP addresses. Otherwise, the administrator must manually assign a unique IP address every time a computer is added to a corporate network. If a client moves from one subnet to another, DHCP can make the appropriate adjustments to a client's IP configuration. This option is enabled by default.
<b>Enable Smart DNS*</b>	Allows the outbound DNS requests to and corresponding inbound replies from assigned DNS servers only. If a computer sends out a DNS request and the response comes back within five seconds, the communication is allowed. All other DNS packets are dropped. If you disable this setting, you must create a firewall rule that allows UDP traffic for remote port 53 (domain) to use DNS. This option is enabled by default.

Option	Description
<b>Enable Smart WINS</b>	<p>Allows the outbound WINS requests to and the corresponding inbound replies from assigned WINS servers only.</p> <p>If a computer sends out a WINS request and the response comes back within five seconds, the communication is allowed. All other WINS packets are dropped.</p> <p>If you disable this setting, to use WINS you must create a firewall rule that allows UDP packets on remote port 137.</p> <p>WINS provides a distributed database that registers and queries dynamic mappings of NetBIOS names for the computers and the groups that a network uses. WINS maps the NetBIOS names to the IP addresses. WINS is used for NetBIOS name resolution in the routed networks that use NetBIOS over TCP/IP. The NetBIOS names are a requirement to establish networking services in earlier versions of Microsoft operating systems. The NetBIOS naming protocol is compatible with network protocols other than TCP/IP, such as NetBEUI or IPX/SPX. However, WINS was designed specifically to support NetBIOS over TCP/IP (NetBT). WINS simplifies the management of the NetBIOS namespace in TCP/IP-based networks.</p> <p>This option is enabled by default.</p>
<b>Allow token ring traffic</b>	<p>Allows the clients that connect through a token ring adapter to access the network, regardless of the firewall rules on the client.</p> <p>If you disable this setting, any traffic that comes from the computers that connect through a token ring adapter cannot access the corporate network. The firewall does not filter token ring traffic. It either allows all token ring traffic or blocks all token ring traffic.</p> <p>This option is disabled by default.</p>
<b>Enable NetBIOS protection</b>	<p>Blocks the NetBIOS traffic from an external gateway.</p> <p>You can use Network Neighborhood file and printer sharing on a LAN and protect a computer from NetBIOS exploits from any external network. This option blocks the NetBIOS packets (UDP 88, UDP 137, UDP 138, TCP 135, TCP 139, TCP 445, and TCP 1026) that originate from IPv4 and IPv6 addresses that are not part of the defined ICANN internal ranges.</p> <p><b>Note:</b> NetBIOS protection can cause a problem with Microsoft Outlook if the client computer connects to a Microsoft Exchange Server that is on a different subnet. You might want to add the IP address of the server to the list of computers that intrusion prevention excludes. Symantec Endpoint Protection processes the excluded computers list before it processes the built-in rules.</p> <p>This option is disabled by default.</p>
<b>Enable reverse DNS lookup</b>	<p>Lets the firewall perform a reverse DNS lookup on IP addresses and compare the domain name with the domain name defined in a firewall rule. Applies only to rules that use domain names in their host definitions.</p> <p><b>Note:</b> This option should be enabled if you use any DNS firewall rules. If this option is disabled, the firewall cannot apply a DNS rule to traffic that uses the IP address of the domain. Typically, it is more secure to specify IP addresses rather than domain names in firewall rules.</p> <p>When this option is enabled, the client computer might experience an impact to performance if response from the DNS servers is slow.</p> <p>This option is disabled by default.</p>

\*These options are the only ones that are supported on Mac clients.

## Protection and Stealth Settings

The stealth settings are not available for the Mac firewall.

**Table 501: Protection and stealth settings**

Option	Description
<b>Enable port scan detection</b>	Monitors all incoming packets that any security rule blocks. If a rule blocks several different packets on different ports in a short period of time, Symantec Endpoint Protection creates a Security log entry. Port scan detection does not block any packets. You must create a security policy to block traffic when a port scan occurs.
<b>Enable denial of service detection</b>	Denial of service detection is a type of intrusion detection. When it is enabled, the client blocks traffic if it detects a pattern from known signatures, regardless of the port number or type of Internet protocol.
<b>Enable anti-MAC spoofing</b>	Allows the inbound and outbound traffic only if a request was made to that specific host for the following protocols: <ul style="list-style-type: none"> <li>• Address Resolution Protocol (ARP)</li> <li>• Neighbor Discovery Protocol (NDP)</li> </ul> It blocks all other unexpected traffic of these type and logs it in the Security Log. Media Access Control (MAC) addresses are the hardware addresses that identify the computers, the servers, and the routers. Some hackers use MAC spoofing to try to hijack a communication session between two computers. When computer A wants to communicate with computer B, computer A may send a packet to computer B. Anti-MAC spoofing protects a computer from letting another computer reset a MAC address table. For example, if a computer sends an ARP REQUEST message, the client allows the corresponding ARP RESPOND message within a period of 10 seconds. The client rejects all unsolicited ARP RESPOND messages. This option is disabled by default.
<b>Automatically block an attacker's IP address</b>	Automatically blocks the IP address of a known intruder for a configurable number of seconds.
<b>Enable stealth mode Web browsing</b>	Detects the HTTP traffic from a web browser on any port. It removes the browser name and version number, the operating system, and the reference web page. It stops websites from detecting which operating system and browser the computer uses. It does not detect HTTPS (SSL) traffic. <b>Warning!</b> Stealth mode web browsing may cause some websites to not function properly. Some web servers build a web page that is based on information about the web browser. Because this option removes the browser information, some web pages may not appear properly or at all. Stealth mode web browsing removes the browser signature, called the HTTP_USER_AGENT, from the HTTP request header and replaces it with a generic signature. This option is disabled by default.

Option	Description
<b>Enable TCP resequencing</b>	<p>Prevents an intruder from forging or spoofing an individual's IP address.</p> <p>IP spoofing is a process that hackers use to hijack a communication session between two computers, such as computer A and B. A hacker can send a data packet that causes computer A to drop the communication. Then the hacker can pretend to be computer A and communicate with and attack computer B. To protect the computer, TCP resequencing randomizes TCP sequence numbers.</p> <p><b>Note:</b> OS fingerprint masquerading works best when TCP resequencing is enabled.</p> <p><b>Warning!</b> TCP resequencing changes the TCP sequencing number when the client service runs. The sequencing number is different when the service runs and when the service does not run. Therefore, network connections are terminated when you stop or start the firewall service. TCP/IP packets use a sequence of session numbers to communicate with other computers. When the client does not run, the client computer uses the Windows number scheme. When the client runs and TCP resequencing is enabled, the client uses a different number scheme. If the client service suddenly stops, the number scheme reverts back to the Window number scheme and Windows then drops the traffic packets. Furthermore, TCP resequencing may have a compatibility issue with certain NICs that causes the client to block all inbound traffic and outbound traffic.</p> <p>This option is disabled by default.</p>
<b>Enable OS fingerprint masquerading</b>	<p>Prevents a program from detecting the operating system of a client computer. The client changes the TTL and identification value of TCP/IP packets to prevent a program from identifying an operating system.</p> <p><b>Note:</b> OS fingerprint masquerading works best when TCP resequencing is enabled.</p> <p><b>Warning!</b> TCP resequencing may have a compatibility issue with certain NICs that causes the client to block all inbound traffic and outbound traffic.</p> <p>This option is disabled by default.</p>

## Peer-to-Peer Authentication Settings

Peer-to-peer authentication blocks a remote computer from connecting to a client computer until the client computer has authenticated that remote computer.

**Table 502: Peer-to-peer authentication settings**

Option	Description
<b>Enable peer-to-peer authentication</b>	<p>Enables the peer-to-peer authentication.</p> <p>The default value is unchecked.</p>
<b>Maximum number of authentication attempts per session</b>	<p>The number of times the client computer challenges the remote computer for a response. The client computer sends the challenge when it does not receive a response from the remote computer. The authentication of the remote computer to the client computer fails after this number is exceeded.</p> <p>The default value is three tries.</p>
<b>Time between authentication attempts (seconds)</b>	<p>The time interval between two consecutive authentication tries.</p> <p>The default value is three seconds.</p>
<b>Time interval after which the remote computer can be reauthenticated (seconds)</b>	<p>The number of seconds that must pass after which the remote computer is allowed to reauthenticate with the client computer.</p> <p>The default value is 30 seconds.</p>
<b>Time that the rejected remote computer is blocked (seconds)</b>	<p>The number of seconds during which the rejected remote computer is blocked from authenticating with the client computer.</p> <p>The default value is 30 seconds.</p>

Option	Description
<b>Time interval of inactivity between the authenticated computer and the client after which the session ends (seconds)</b>	The time limit for inactivity between the two computers, in seconds, after which the session is closed. The default value is 40 seconds.
<b>Exclude hosts from authentication</b>	The hosts you want to exclude from authentication and for which to allow traffic.

## Network Application Monitoring for <group name>

You can configure whether the client computer monitors the applications that try to access the network.

**Table 503: Network application monitoring options**

Option	Description
<b>Enable network application monitoring</b>	Enables the client to monitor changes to applications that run on the client computer.
<b>When an application change is detected</b>	Specifies the action that the firewall should take on an application that the client detects has changed. The following actions are available: <ul style="list-style-type: none"> <li>• <b>Ask</b></li> <li>• <b>Block the traffic</b></li> <li>• <b>Allow and Log</b></li> </ul>
<b>Additional text to display</b>	Adds the text to the standard message that appears on the client computer if the client detects that an application has changed.  <b>Note:</b> The operating system limits the amount of text that can be displayed in this notification on the client computer. To avoid the truncation of the notification text, you should limit your added text to no more than 120 characters.
<b>Unmonitored Application List</b>	Displays a list of applications that the client does not monitor.
<b>Enabled</b>	Enables the client to ignore the applications that change on the client computer. Uncheck this check box when you want to monitor an application that appears in this list.  <b>Note:</b> This check box appears only when there are applications in the list.
<b>Add</b>	Enables you to define an application to monitor.
<b>Add From</b>	Enables you to define an application to monitor by filtering the applications in the learned applications list.

## Intrusion Prevention System Policy

### Excluded Hosts

You may need the IPS signatures to ignore the traffic that goes to and from certain client computers. For example, some computers in your internal network may be set up for testing purposes.

Excluded hosts do not require peer-to-peer authentication. When the authenticator client receives new inbound traffic from a remote client, the authenticator first checks whether the remote client is in the **Excluded Hosts** list. If the remote client is in the list, the authenticator allows the traffic and does not start peer-to-peer authentication.

#### NOTE

Excluded hosts is supported for network intrusion prevention only.

**Table 504: Excluded hosts**

Option	Description
Enabled	<b>When Enabled is checked, it causes the following actions:</b> <ul style="list-style-type: none"><li>• Intrusion prevention ignores traffic to and from the specified computer.</li><li>• Peer-to-peer authentication does not start on the specified computer.</li></ul> <b>When Enabled is unchecked, it causes the following actions:</b> <ul style="list-style-type: none"><li>• Intrusion prevention checks traffic to and from the specified computer.</li><li>• Peer-to-peer authentication starts on the specified computer.</li></ul> If you add a host from the <b>Policy Components</b> list, you can enable it and disable it. If you add a host by clicking <b>Add</b> , the host is automatically enabled. To disable the host, remove it from the list.
Group Name	Lists the name of a group of hosts. This field appears only if you added a group of hosts from the <b>Policy Components</b> list. You cannot edit host groups; you can only enable or disable them.
Content	Defines the host type and content.

## Exceptions

Use this table to view and configure IPS signature exceptions for Windows computers or Mac computers. You can create exceptions for signatures, which are downloaded to the client as part of LiveUpdate content. The signatures do not appear in the policy until the management server downloads content from LiveUpdate. For Mac computers, you can also create exceptions for several built-in signatures that are available after you install the management server.

For network signatures, you can change the default action and the log action. You might want to change the default action and the log action before you download the network signatures to the client.

### NOTE

You cannot change the default behavior for browser signatures. Browser signatures are supported on Windows only.

If you want to remove an exception, select it and then click **Delete**. If you edit the behavior so that the behavior is the same as the network signature's original behavior, the signature remains in the exceptions list.

**Table 505: Exceptions options**

Option	Description
ID	The ID that Symantec assigns to each signature.
Signature Name	The name of signature.
Severity	The level of danger that the traffic packet causes if the signature detects it.
Categories	Type of signature.
Action	The action that the client takes on the traffic packet that matches the IPS signature.
Log	The logging action that the client takes on the traffic packet that matches the IPS signature.

## Intrusion Prevention settings

Use this page to enable or disable the intrusion prevention settings for the client.



## NOTE

A lock icon appears next to some options. Click the icon to lock or unlock an option on client computers. When you lock an option, you prevent user changes to the option.

**Table 506: Intrusion prevention options**

Option	Description
<b>Enable Network Intrusion Prevention</b>	<p>Applies the network IPS signatures, exceptions to IPS signatures, and IPS custom signatures to the inbound and the outbound traffic on the client.</p> <p>Network attacks are logged in the Security log. You can configure notifications to appear if the client computer detects an attack.</p> <p>Typically, you should always enable this option. This option is enabled by default.</p> <p><b>Enable excluded hosts:</b> Enables a list of computers for which the client ignores all inbound and all outbound traffic. The client does not apply the firewall rules or match IPS signatures to the computers in the list. The client also does not check these computers for port scans, anti-MAC spoofing, or denial-of-service attacks.</p>
<b>Enable Browser Intrusion Prevention for Windows</b>	<p>Applies the IPS web browser signatures to the inbound and the outbound browser traffic on the client.</p> <p><b>Note:</b> This option is only supported on the Symantec Endpoint Protection clients that run Windows.</p> <p>When this option is enabled, the client compares the browser signatures to the inbound and the outbound traffic from browsers.</p> <p>Supported browsers include Internet Explorer and Firefox. The Google Chrome browser extension is installed by default in 14.3 RU1 and later. Other browsers are not supported. For information about specific browser versions, see:</p> <p><a href="#">Supported browsers for Browser Intrusion Prevention in Endpoint Protection</a></p> <p>Browser attacks are logged in the Security log.</p> <p>For some browser attacks, intrusion prevention requires that the client terminate the browser. A notification appears on the client computer.</p> <p>Typically, you should always enable this option. This option is enabled by default.</p> <p><b>Log detections but do not block:</b> Use this option when you want to observe the detections that Browser Intrusion Prevention makes before you start blocking browser intrusion detections. Typically you should disable log-only mode after a short period of time to provide the best protection on your client computers.</p>
<b>Enable URL reputation</b>	<p>Identifies threats from domains and URLs, which can host malicious content like malware, fraud, phishing, and spam, etc. URL reputation blocks access to the web addresses that are identified as known sources of the malicious content. The information from visited URLs is scored. Web pages with reputation scores below a specific threshold are considered threats and blocked.</p> <p>URL reputation requires SymPlatform definitions and IPS definitions downloaded from Symantec LiveUpdate.</p> <p>URL reputation allows any websites that you specify as a Trusted Web Domain Exception.</p> <p>Available in 14.3 RU1.</p>
<b>Out-of-band scanning</b>	<p>Multi-threaded network scanning. Applies to network intrusion prevention.</p> <p>Supported for Windows 8.1 and later. Especially recommended for servers due to the high throughput environment.</p> <p><b>Note:</b> This mode changes the processing model for networking traffic and may have compatibility issues with other Windows Filtering Platform (WFP) drivers. Therefore, if you enable this option, Symantec recommends that you test out-of-band scanning before you deploy it to your production environment. Performance characteristics vary depending on the workload.</p>
<b>Use signature subset for servers</b>	<p>Uses a subset of intrusion prevention signatures for the most common activity that is seen on server operating systems. Applies to network intrusion prevention and browser intrusion prevention.</p>

---

## Add Intrusion Prevention Exceptions

Use this dialog to change the default behavior of intrusion prevention signatures on the client. On Windows computers, the signatures list matches the list of signatures that LiveUpdate downloads to your clients. On Mac computers, some signatures are built into the client software. LiveUpdate content must be available on the management server to display the signature list in the policy. Otherwise, for Windows computers, the list is empty, and for Mac computers, the list contains only the built-in signatures.

You can change the default actions that the client takes if the selected signature detects a traffic packet that matches the signature. The client allows or blocks the traffic packet and logs or does not log the information about the traffic packet.

For Windows computers, audit signatures are also included so that you can monitor certain types of traffic, such as Yahoo IM logons. By default, these signatures are set to **Not log**. You can create an exception to log this traffic and then check the logs and decide how to handle the traffic. For example, you might want to create a firewall rule for that traffic type.

You can filter the signatures based on the category or the level of severity.

### NOTE

If you select multiple signatures at the same time, you cannot specify more than one action. For example, either the client blocks all the selected events, or the client allows all the selected events.

**Table 507: Intrusion prevention signature contents**

Option	Description
<b>Show category</b>	Applies to Windows exceptions only. Types of signatures that you can filter on. The default is <b>All</b> .
<b>Show severity</b>	Level of the severity that is associated with each signature. The default is <b>All</b> .
<b>ID</b>	ID that Symantec assigns to each signature.
<b>Signature Name</b>	Name of signature. Audit signatures include the word <b>Audit</b> in the name. Audit signatures are supported only on Windows computers.
<b>Severity</b>	Level of the danger that the traffic packet causes if the signature detects it.
<b>Categories</b>	Type of signature. For Mac clients, the <b>Category</b> also includes <b>Built-in</b> .
<b>Action</b>	Allows or blocks the traffic packet.
<b>Log</b>	Logs or does not log information about the packet.
<b>Select All</b>	Selects all signatures in the list.
<b>Unselect All</b>	Deselects all signatures in the list.

Select one or more signatures in the list, and then click **Next** to select the action and specify the log option.

## Signature Action

You can change the response that the client takes when a Symantec IPS network signature matches and detects an event. For example, if the default action is to block the event, you can allow it. If the default action is to allow the event, you can block it.

---

## NOTE

You cannot change the allow or block response for browser signatures. When you add an exception for a browser signature, Symantec Endpoint Protection Manager automatically configures the signature with the action and logging settings as **Allow** and **Do Not Log**.

**Table 508: Signature actions**

Option	Description
<b>Action</b>	Specifies one of the following actions that the client takes on the traffic event: <ul style="list-style-type: none"><li>• <b>Block</b> Prevents the traffic from accessing the client This is the default action.</li><li>• <b>Allow</b> Ignores the traffic</li></ul>
<b>Log</b>	Logs or does not log the traffic event in the Security Log and Traffic Log. The default is <b>Log the traffic</b> .

## Custom Intrusion Prevention Signatures: Signatures

Use this tab to add signature groups and signatures to a custom IPS library. You must create a signature group before you can add signatures.

**Table 509: IPS library signature options**

Option	Description
Name	The name of the Custom Intrusion Prevention Library.
Description	The description of the Custom Intrusion Prevention Library.
Signature Groups	The available signature groups. You can add and delete the signature groups that are in this list. The default Custom Intrusion Prevention Library includes a default signature group.
Group Name	The name of the signature group. Use this text field to edit the group name.
Description	The optional description of the signature group. Use this text field to edit the description.
Enable this group	The way to activate the signature. You must enable the signature group to activate all the signatures in it. Signature groups are enabled by default.

Option	Description
Signatures for this Group	<p>The signatures and the signature content for each signature group. You can add, edit, or delete a signature in this list, as well as configure the following options:</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b> Activates the signature.</li> <li>• <b>Name</b> The name of the signature.</li> <li>• <b>Content</b> The signature syntax.</li> <li>• <b>Applications</b> An application that triggers a custom IPS signature.</li> <li>• <b>Action</b> The action the client takes on the traffic packet if its signature matches the IPS signature.</li> <li>• <b>Track</b> Logs the event in the Packet Log.</li> <li>• <b>Move Up and Move Down</b> Moves the selected signature up one row or down one row. You move a signature to change the order that the signature is processed. The IPS engine for custom signatures checks each signature in the order that they are listed in the signatures table. Only one signature is triggered per packet. When a signature matches an inbound or an outbound traffic packet, the IPS engine stops checking other signatures. Custom signatures must be executed in the correct order. Therefore, you may want to change the order of the signatures. If multiple signatures match, you should move the higher priority signatures to the top.</li> </ul>

## Intrusion Prevention Signature Group

Use this dialog box to add a name and optional description for a signature group.

## Add Application or Edit Application

Use this dialog box to define an application that triggers a custom IPS signature.

Add an application to the list by typing its name and an optional description. When you add the file name, you can use either format: `iexplore` or `iexplore.exe`. You can later edit the application's information or delete it from the list.

If you want any application to trigger the signature, type the wildcard character `*`.

## Custom Intrusion Prevention Signatures: Variables

When you add signatures to a custom IPS library, you can use variables to represent changeable data, or values, in signatures. If the data changes, you can edit the variable instead of editing the signatures throughout the library.

The variables that you define in the custom IPS signature library can be used in any signature in that library. You can add, edit, or delete variables from this list, by using the options.

**Table 510: Variables tab**

Option	Description
Enabled	<p>Activates the variable.</p> <p>If you don't enable a variable, the signature ignores the variable when the variable is used in a custom signature.</p>
Name	Name of the variable, such as <code>ip</code> .

Option	Description
Description	Shows how the variable is used in the signature, such as: <ul style="list-style-type: none"> <li>var ip=(192.10.58.10/24) (IPv4)</li> <li>var ip=(fd15:4ba5:5a2b:1008::/64) (IPv6)</li> </ul>
Content	Contains the content string for the variable value, up to 255 characters. Use the following format: <ul style="list-style-type: none"> <li>(0.0.0.0/0) (IPv4)</li> <li>(fd15:4ba5:5a2b:1008::/64) (IPv6)</li> </ul> Use the following syntax: <pre>rule protocol-type, [protocol-options,] [ip-protocol options,] msg, content...</pre>

[Syntax for custom intrusion prevention signatures](#)

[Defining variables for custom IPS signatures](#)

## Add Variable or Edit Variable

Use this dialog box to add or edit the variables that are used when you write custom signatures.

**Table 511: Add Variable or Edit Variable tab**

Option	Description
Name	Lists the name of the variable, such as ip.
Description	Describes how the variable is used in the signature, such as var ip=(192.10.58.10/24).
Content	Displays the content of the variable. The maximum value of the variable is 255 characters. Use the following format: (0.0.0.0/0) Use the following syntax: <pre>rule protocol-type, [protocol-options,] [ip-protocol options,] msg, content...</pre>

[Syntax for custom intrusion prevention signatures](#)

[Defining variables for custom IPS signatures](#)

## Custom Intrusion Prevention for Group name

Use this dialog box to assign custom Intrusion Prevention signatures to the selected group. You can assign multiple sets to the group. The custom signatures must be enabled for the management server to download the signatures to the clients in the group.

The custom IPS signatures table displays the name and description of each library and the date and time that you created the library.

## Add Signature or Edit Signature

Use this dialog box to write your own packet-based signatures to add to a custom IPS library.

**Table 512: Add Signature or Edit Signature dialog box**

Options	Description
Name	The name of the custom signature.
Description	The description of the custom signature.
Severity	The severity of the event that triggers the signature.
Direction	The direction of the event traffic that the signature checks.
Content	<p>The text box where you enter the signature syntax.</p> <p>Use the following syntax. Arguments that are followed by an ellipsis may be repeated.</p> <pre>rule protocol-type, [protocol-options,] [ip-protocol options,] "msg", "content"...</pre> <ul style="list-style-type: none"> <li>rule protocol-type, [protocol-options,] [ip-protocol option,] = The traffic description.</li> <li>msg = The text string that appears in the security log. The message string must be enclosed in double quotes (" "). Single quotes (') are not allowed.</li> <li>content = The string that is matched against the payload component in the packet for a possible match. The content string must be enclosed in double quotes (" "). Single quotes (') are not allowed.</li> </ul>
Applications	<p>The applications that trigger the signature. By providing the application names, you can help reduce the false positives that other applications may generate.</p> <p>You must check the <b>Enabled</b> check box for the application to trigger the signature. If you want any application to trigger the signature, type the wildcard character *.</p>
Action	<p>The actions that can occur when the event or attack is triggered.</p> <ul style="list-style-type: none"> <li>Block Identifies and blocks the event or attack and records it in the client's security log. Use this action when the severity is high.</li> <li>Allow Identifies and records the event or attack in the client's security log. Use this action to monitor traffic.</li> <li>Write to Packet Log Records the event or attack in the client's packet log. The Packet log contains a dump of the transaction.</li> </ul>

[Managing custom intrusion prevention signatures](#)

[Syntax for custom intrusion prevention signatures](#)

## Regular expressions in custom IPS signature content and application control rules

You can use regular expressions (regex) in custom IPS signature content and application control rules. The usage of regular expressions can differ from standard usage.

### Custom IPS regular expressions

For custom IPS, regular expressions use the following format:

```
regexcontent="string value" (offset, depth)opt
```

offset	Specifies the start of the bytes in the packet data, from which the IPS engine matches the signature pattern.
depth	Specifies the length of the packet data in which the IPS engine matches the signature pattern.

opt	Includes the C and the H options. <ul style="list-style-type: none"> <li>• The C option makes the expression not case-sensitive.</li> <li>• The H option specifies HTTP decoding.</li> <li>• If there is no option, the entire data packet is matched.</li> </ul>
-----	---

### For custom IPS, regular expressions support the following characteristics:

- Multiple regexcontent
- Case-sensitivity
- Binary format

The format is `\x` or `\X` with two Hex digits, like `\xA9`.

### Application control regular expressions

Regular expressions for application control are not case-sensitive.

For application control, some syntax differs from common regular expression syntax. Some common regular expression features are not supported. In addition, unique application control features can be used in the regex pattern.

Application control regular expression syntax differs from standard syntax in the following ways:

- Escaped parentheses define a group. Unescaped parentheses are interpreted as literal characters.
- The beginning anchors and end anchors are added automatically. If you add them manually into the expression, they are treated as literal characters.

The table [Syntax for regular expressions for custom IPS and application control](#) provides examples of these differences.

Certain common features for regular expressions are not supported, such as:

- The character classes `\d`, `\w` and `\s`, and the reverse versions `\D`, `\W`, and `\S`.  
Instead, use alphanumeric sets, such as `[0-9]` instead of `\d`, or `[a-z0-9_]` instead of `\w`.
- The curly bracket quantifiers `{nn}` and `{nn,nn}`.  
Instead, repeat the desired pattern. For example, use `[XYZ][XYZ][XYZ]` instead of `[XYZ]{3}`.
- The optional quantifier `?`, which represents "zero or one".  
You may be able to use `*` in some cases.

Unique application control features you can use in regular expressions include:

- Importing registry value strings with `#`.  
For example, `#HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir#\Messenger\msmsgs.exe` can match `msmsgs.exe` on a localized operating system where Program Files is named differently.
- Importing environmental variable strings with `%`.  
For example `%windir%\winhlp32.exe` matches `winhlp32.exe` in the Windows folder, even if it is named differently or is located on an alternate drive.

#### NOTE

To match the literal character `%`, use `%%`.

### Syntax for regular expressions

**Table 513: Syntax for regular expressions for custom IPS and application control**

Symbol	Description
Character	Matches itself, unless it is one of the following special characters (metacharacters): <ul style="list-style-type: none"> <li>Custom IPS: . \ [ ] * + ^ \$</li> <li>Application control: . \ [ ] * +</li> </ul>
.	Matches any one character.
\	Matches the character following it, except when followed by: <ul style="list-style-type: none"> <li>A left parenthesis or a right parenthesis: ( )</li> <li>A left angle bracket or right angle bracket: [ ]</li> <li>A digit from 1 to 9</li> </ul> The \ character is used as an escape character for all other metacharacters as well as itself. When it is used in a set, the \ character is treated as an ordinary character.
[set] [^set]	Matches one of the characters in the set. If the first character in the set is ^, it matches a character that is not in the set, i.e., it complements the set. A shorthand S-E is used to specify a set of characters S up to E, inclusive. The special characters ] and - have no special meaning if they appear as the first characters in the set. For example: <ul style="list-style-type: none"> <li>[a-z]: Matches any alphabetic character.</li> <li>[^]-]: Matches any character except ] and -.</li> <li>[^A-Z]: Matches any character except alphabetical characters (uppercase alphabetical characters for IPS).</li> <li>[a-zA-Z]: Matches any alphabetic character. It is the same as [a-z] or [A-Z].</li> </ul>
*	Any regular expression from the first four rows of this table, followed by a closure character (*), that matches zero or more matches of that form.
+	Same as *, except that + matches one or more matches of that form.
\(form\)	A regular expression in supported syntax \ (form\ ) matches whatever form matches. The enclosure tags the form to be used with \single digit for pattern substitution, where single digit is a number from 1 to 9. The tagged forms are numbered in sequence starting at the beginning of the syntax. For example: <ul style="list-style-type: none"> <li>\ (xxx\ ) [1-3] matches xxx1 or xxx2 or xxx3</li> </ul> Unescaped parentheses are interpreted as literal characters. For example: <ul style="list-style-type: none"> <li>C:\Program Files (x86)\test\test.exe correctly matches searches within C:\Program Files (x86).</li> </ul>
\single digit	Matches whatever a previously tagged \ (form\ ) matched. The digit indicates which tagged form to match as a substitution. Note that the parentheses are escaped with a backslash. Unescaped parentheses are interpreted literally. In the first example here, \ (xxx\ ) is tagged as 1. In the second example, \ (yy\ ) is tagged as 1, (zz\ ) is tagged as 2. <ul style="list-style-type: none"> <li>\ (xxx\ ) [1-3] \1 matches xxx1xxx or xxx2xxx or xxx3xxx</li> <li>\ (yy\ ) X \ (zz\ ) [1-3] \2 \1 matches yyXzz1zzyy or yyXzz2zzyy or yyXzz3zzyy</li> </ul>
\< \>	A regular expression that starts with \< restricts the pattern matching to the beginning of a word. A regular expression that ends with \> restricts the pattern matching to the end of a word. You can use these symbols together or separately. A word is defined to be a character string that begins and/or ends with the characters A-Z a-z 0-9 and _. Any character outside those mentioned must precede or follow it. For example, the syntax: .* \<Symantec.\>.* matches ...ABC Symantec 123....



Symbol	Description
^ \$	<p>A regular expression that starts with ^ and/or ends with \$. These anchor characters restrict the pattern matching to the beginning of the line, or to the end of line. Elsewhere in the pattern, ^ and \$ are treated as ordinary characters. For application control, you do not need to add these anchor characters. They are automatically added to the beginning and the end of the search term. If you add these characters, they are interpreted literally.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>c:\\file\\.txt matches c:\file.txt, but c:\\file\\.txt\$ does not.</li> <li>.*\\notepad\\.exe matches notepad.exe in any folder, but notepad\\.exe does not match notepad.exe in any folder. The automatically added anchor characters mean that it does not match the full path of the file.</li> </ul>

[Syntax for custom intrusion prevention signatures](#)

## Syntax for custom intrusion prevention signatures

### About signature syntax and conventions

When you write the content for each IPS signature, you must use the following syntax:

```
rule protocol-type, [protocol-options,] [ip-protocol options,] "msg", "content"...
```

You must begin each signature with the keyword `rule`, followed by the protocol type argument, protocol options, IP protocol options, msg arguments, and content arguments. The optional arguments are enclosed in square brackets. Type only the information within the brackets; do not type the brackets. Arguments that are followed by an ellipsis may be repeated. You provide the information for the arguments, by using the supported operators and the regular expressions.

### Protocol type arguments

This part of the signature defines the protocol type by using the following syntax:

```
protocol-type
```

**where protocol-type is one of the following parameters:**

- tcp
- udp
- icmp

The protocol type must immediately follow the word `rule`.

For example:

```
rule udp
```

Each `tcp`, `udp`, and `icmp` protocol type supports its own set of optional arguments.

### TCP protocol arguments

For additional details on the TCP protocol, refer to RFC 793:

<https://tools.ietf.org/html/rfc793>

**Table 514: TCP protocol arguments**

Attribute	Description	Syntax
source	Source TCP port	<code>source operator (value)</code> where <code>value</code> is an unsigned 16-bit number from 0 to 65535. Example: <code>source=(180,2100)</code> The value must be enclosed in parentheses. A value of 0 (zero) indicates all ports. You can specify a range of ports by using a dash between two port values (for example 3-5 is ports 3, 4, and 5). Multiple ports can be specified by separating them with commas.
dest	Destination TCP port	<code>dest operator (value)</code> where <code>value</code> is an unsigned 16-bit number from 0 to 65535. For example: <code>dest=(120,125)</code> The value must be enclosed in parentheses. A value of 0 (zero) indicates all ports. A range of ports can be specified by using a dash between two port values (for example 3-5 is ports 3, 4, and 5). Multiple ports can be specified by separating them with commas.
tcp_flag	TCP flags present in the packet	<code>tcp_flag operator flag [flag]...</code> where <code>flag</code> is one of the following parameters: <ul style="list-style-type: none"><li>• <code>fin</code>: end of data</li><li>• <code>syn</code>: synchronize sequence numbers</li><li>• <code>rst</code>: reset connection</li><li>• <code>psh</code>: push function</li><li>• <code>ack</code>: acknowledgement field significant</li><li>• <code>urg</code>: urgent pointer field significant</li><li>• <code>0</code>: match all flags</li></ul> For example: <code>tcp_flag&amp;ack ps</code> Most <code>tcp_flag</code> tests use the <code>&amp;</code> (bitwise and) operator as a mask (meaning that a packet must have the specified flags set but can also have other flags set). You can specify multiple flags in a test by placing a pipe character ( <code> </code> ) between the flags.
window	TCP window size	<code>window operator size</code> where <code>operator size</code> is an unsigned 16-bit number from 0 to 65535. For example: <code>window=16384</code>

## UDP protocol arguments

For additional details on UDP protocol, refer to RFC 768:

<https://tools.ietf.org/html/rfc768>

**Table 515: UDP protocol arguments**

Attribute	Description	Syntax
source	Source UDP port	<code>source operator (value)</code> where <code>value</code> is an unsigned 16-bit number from 0 to 65535. For example: <code>source=(180,2100)</code> The value must be enclosed in parentheses. A value of 0 (zero) indicates all ports. A range of ports can be specified by using a dash between two port values (for example 3-5 is ports 3, 4, and 5). Multiple ports can be specified by separating them with commas.
dest	Destination UDP port	<code>dest operator (value)</code> where <code>value</code> is an unsigned 16-bit number from 0 to 65535. For example: <code>dest=(120)</code> The value must be enclosed in parentheses. A value of 0 (zero) indicates all ports. A range of ports can be specified using a dash between two port values (for example 3-5 is ports 3, 4, and 5). Multiple ports can be specified by separating them with commas.

### ICMP protocol arguments

Refer to RFCs 792 and 1256 for detailed descriptions of valid ICMP protocol type and code combinations:.

- <https://tools.ietf.org/html/rfc792>
- <https://tools.ietf.org/html/rfc1256>

ICMPv4 and ICMPv6 are supported for ICMP rules.

ICMPv6 is supported as of version 14.2.

**Table 516: ICMP protocol arguments**

Attribute	Description	Syntax
type	ICMP protocol type	<code>type operator value</code> where <code>value</code> is an unsigned 8-bit number from 0 to 255. For example: <code>type=0</code>
code	ICMP protocol type	<code>code operator value</code> where <code>value</code> is an unsigned 8-bit number from 0 to 255. For example: <code>code&lt;=10</code>

### IP protocol arguments

The IP protocol arguments are independent of the protocol type arguments and are valid for the TCP, UDP, and ICMP protocol types.

For additional details on IP protocol, refer to RFC 791:

**Table 517: IP protocol arguments**

Attribute	Description	Syntax
saddr	Source IP address	<p>saddr=(value/CIDR)  where:</p> <ul style="list-style-type: none"> <li>value is an IPv4 or IPv6 address that specifies the IP address of the computer that runs the client, or the variable \$LOCALHOST.  IPv6 is supported as of version 14.2.</li> <li>CIDR is a classless inter-domain routing notation that indicates how many bits are used for the network prefix.</li> </ul> <p>For example:  saddr=(127.0.0.0/25)  Here, 25 bits of the IPv4 address are used to identify the unique network and the remaining bits that identify the host.  saddr=(2001:0db8::0001/32)  Here, 32 bits of the IPv6 address are used to identify the unique network and the remaining bits that identify the host.</p>
daddr	Destination IP address	<p>daddr=(value/CIDR)  where:</p> <ul style="list-style-type: none"> <li>value is an IPv4 or IPv6 address that specifies the IP address of the computer that runs the client, or the variable \$LOCALHOST.  IPv6 is supported as of version 14.2.</li> <li>CIDR is a classless inter-domain routing notation that indicates how many bits are used for the network prefix.</li> </ul> <p>For example:  daddr=(128.0.0.0/4)  Here, four bits of the IPv4 are used to identify the unique network and the remaining bits that identify the host.  daddr=(2001:0db8::0002/120)  Here, 120 bits of the IPv6 address are used to identify the unique network and the remaining bits that identify the host.</p>
tos	Type of service flag present in the packet This attribute applies only to IPv4 addresses.	<p>tos operator value  where value is a numeric constant in a decimal, hexadecimal, or octal format.  For example:  tos=0x4  To view valid IP tos values, see <a href="#">Valid IP tos values</a>.  To test for multiple IP tos values in a packet, the tos argument should be the sum of the values that are to be tested. Typically, the operator is either = or &amp;. You cannot combine these flags using the pipe character (   ).</p>

Attribute	Description	Syntax
tot_len	Total length of the packet This attribute applies only to IPv4 addresses.	<code>tot_len operator value</code> where <code>value</code> is a 16-bit number from 0 to 65535 that specifies the total length of packet. For example: <code>tot_len&gt;1445</code> When you specify the value, the rule protocol-type must be considered to properly calculate the length to be tested. To aid in calculating the <code>tot_len</code> for each of the supported protocol types, their header lengths are as follows: TCP: 20-60 bytes UDP: 8 bytes ICMP: 8-20 bytes
ttl	Time-to-live (TTL) of the packet This attribute applies only to IPv4 addresses.	<code>ttl operator value</code> where <code>value</code> is an 8-bit value from 0 to 255 that specifies the time-to-live characteristic of the packet.
ip_flag	Fragmentation offset value of the packet This attribute applies only to IPv4 addresses.	<code>ip_flag operator value</code> where <code>value</code> is a 13-bit value that specifies the fragmented offset value in the packet. IP fragmentation offsets occur on 8-byte boundaries; therefore, each bit value in the fragmentation offset represents three bits.

**Table 518: Valid IP tos values**

Dec	Hex	Option
2	0x2	Minimize monetary cost
4	0x4	Maximize reliability
8	0x8	Maximize throughput
24	0x18	Minimize delay

### Msg arguments

When an IPS signature successfully matches packet content with the rule's test conditions, the message is specified in the `msg` argument. The `msg` argument appears in the Security Log on both the client and the server. Only one `msg` argument can be included in each IPS signature.

Syntax:

```
msg="alert message"
```

The alert message must be enclosed in double quotation marks and cannot contain punctuation. Single quotation marks are not allowed. The purpose of the alert message is to let you easily identify an event in your network by reviewing the Security Log. Therefore, all IPS signatures must contain concise yet descriptive alert messages within the `msg` argument.

Example:

```
msg="IIS Unicode Transversal Vulnerability"
```

### Content arguments

The content argument specifies a pattern to look for within a packet. The content argument can appear multiple times in an IPS signature. The content value must be enclosed in double quotation marks ("). Single quotation marks (') are not allowed.

---

## Syntax:

```
content="value"
```

where `value` is a pattern that is specified as a string literal or a binary literal that must be enclosed in quotation marks.

A string literal is a group of consecutive characters, including spaces. A string can contain any characters except a quotation mark (`"`), backslash (`\`), or newline character escape sequence (`\n`). Example:

```
content="system32"
```

A binary literal is a group of consecutive bytes expressed in hexadecimal format, where the escape sequence `\x` precedes each byte. Example:

```
content="\x04\x20\x20\x20\xBF"
```

The following example specifies the content as the binary literal `"\x04\x20\x20\x20\xBF"`.

String literals can be combined with binary literals to create complex patterns. Example:

```
content="\x0DLocation\x3A"
```

## Optional content arguments

You can use additional optional content arguments to further qualify the content in the following ways:

- Case-sensitivity
- HTTP decoding
- Depth and offset

### Case-sensitivity

You can specify an optional C case-sensitivity flag on each content argument. When you use this flag, the content argument pattern string matches only if the case of its characters matches the case of the data in the packet.

For example, you can use the following syntax:

```
content="value"C
```

```
content="\x0DLocation\x3A"C
```

### HTTP decoding

You can use the optional HTTP H decoding flag in each content argument. If you use the H HTTP decoding flag, encoded characters are converted into a binary literal before they try a pattern match. You can also use the HTTP H after a C case-sensitivity flag. HTTP URIs use encoded characters. When the pattern match is attempted and normalized, the normalized data is compared to the binary or the string literal in the content argument. Under most circumstances, the H flag is used only for the TCP rules that relate to an application that uses the HTTP protocol.

For example, you can use the following syntax:

```
content="value"H
```

```
content="\x6f\x6e\x4c\x6f\x61\x64\x3d\x22\x61\x6c\x65\x72\x74\x28"H
```

### Offset and depth

You can use the offset value and a depth value as optional arguments in the content. The offset value is specified first, followed by the depth value.

For example, you can use the following syntax:

```
content="value" (offset,depth)
```

Syntax	Description
value	A pattern that is specified as a string literal or a binary literal that must be enclosed in quotation marks.
offset	<p>A positive integer in decimal notation.</p> <p>The offset specifies an alternative location to begin a pattern match. The offset also specifies how many bytes to skip before the signature tries to pattern match.</p> <p>When an offset argument is not present or has a value of 0, the content argument pattern tries to find a match. The pattern tries to match the one of the following:</p> <ul style="list-style-type: none"><li>• The content at the beginning of the packet payload</li><li>• The portion of the packet following the protocol header for the first content argument</li></ul> <p>Each successive content argument automatically begins to test for pattern matches that follow the end of the previous successful pattern match.</p>
depth	<p>A positive integer in decimal notation. The depth specifies the maximum number of bytes to search when trying to match a pattern in a content argument.</p> <p>When a depth argument has a value of 0, the pattern that is contained in the content argument tries to find a match from the offset to the end of the packet. The depth argument value cannot be smaller than the number of bytes that are specified as the pattern to match within the argument of the content argument.</p>

```
content="\x04\x20\x20\x20\xBF" (4,5)
```

This example skips four bytes forward from the previous pattern match or from the beginning of the packet payload. It then compares the next five bytes with the binary literal that is contained in the content argument.

### Streamdepth arguments

You can use the streamdepth argument to limit the length of the stream in which the intrusion prevention rule checks for a signature. You might want to use streamdepth to improve the performance of your custom intrusion prevention rules. The streamdepth argument is optional.

Syntax:

```
streamdepth=value
```

For example, you might suspect that a signature exists in the first 10KB of a 1MB stream. You can use the following syntax:

```
streamdepth=10240
```

On the file download, the intrusion prevention rule with this streamdepth value stops checking for the signature after 10KB. Since you limit the checking, the download performance is improved.

If you set streamdepth to 0, intrusion prevention applies the rule to the entire stream.

### Supported operators

Many arguments in the signature syntax require an operator that indicates the type of test that is to be performed to check for this type of attempt.

[Supported operators used in IPS signatures](#) describes the supported operators.

**Table 519: Supported operators used in IPS signatures**

Operator	Description
<	Less than
>	Greater than

Operator	Description
=	Equal to
&	Bitwise AND In the signature library, the ampersand character, &, is sometimes represented using its HTML equivalent, &amp;
<=	Less than or equal to
>=	Greater than or equal to

### Sample custom IPS signature syntax

You can create sample custom IPS signatures to detect an attempt to access and download MP3 files through a Web browser or FTP.

The format of an MP3 file makes it difficult to detect an MP3 file in network traffic. However, you can view the TCP packets to find the commands and protocols that are used to retrieve the MP3 files. You can then use this information to create the syntax for a custom IPS signature.

To detect an MP3 file and then block access to it, you write two signatures. One signature detects an MP3 file through the HTTP service. The second signature detects an MP3 files through the FTP service.

When you create a custom IPS signature, you must type the content of the signature by using the following format:

```
rule protocol-type, [protocol-options,] [ip-protocol
option,] msg, content...
```

During an HTTP or FTP session, the server and the client exchange information. The information is contained in the TCP packets that are destined for the appropriate service on the server. The HTTP service uses port 80 and the FTP service uses port 21. The TCP packets contain the required information in a payload component.

Web browsers use the HTTP GET command to download MP3 files. The FTP client uses the FTP RETR command to download files. The FTP command is also used when multiple files are retrieved by using the MGET command. The file name and respective mp3 extension is present in both requests. Both protocols insert [CR][LF] characters to mark the end of the request

The signature syntax must also contain several parameters, including a regular expression that identifies the specific commands that should be blocked. Regular expressions are patterns of the characters that are compared against the contents of the packet. The commands you want to block are contained in these packets. If you do not know the name of a particular file, you can use the wildcard character (\*) to match the unknown number of characters between the command and the file name. The command must be in lower case, but the file extension can be in either case.

### Regular expressions in custom IPS signature content and application control rules

The content of the HTTP signature contains the following syntax:

```
rule tcp, dest=(80,443), saddr=$LOCALHOST,
msg="MP3 GET in HTTP detected",
regexpccontent="[Gg][Ee][Tt] .*[Mm][Pp]3 ."
```

The content of the FTP signature contains the following syntax:

```
rule tcp, dest=(21), tcp_flag&ack, saddr=$LOCALHOST,
msg="MP3 GET in FTP detected",
regexpccontent="[Rr][Ee][Tt][Rr] .*[Mm][Pp]3\x0d\x0a"
```

[HTTP signature and FTP signature syntax](#) explains the syntax for the HTTP signature and the FTP signature.



**Table 520: HTTP signature and FTP signature syntax**

Use the following syntax	To perform the following task
<p>For the HTTP signature:</p> <pre>rule tcp dest=(80,443)</pre> <p>For the FTP signature:</p> <pre>rule tcp dest=(21)</pre>	<p>Tells the packet-based engine what traffic to search. This way, the engine does not search unnecessary traffic and does not use up system resources. The more detailed information you provide, the better the packet-based engine performs.</p> <p>This argument limits the destination ports to 80 and 443 for the HTTP service and to 21 for the FTP service.</p>
<p>For the FTP signature:</p> <pre>tcp_flag&amp;ack</pre>	<p>Reduces the false positives.</p>
<pre>saddr=\$LOCALHOST</pre>	<p>Makes sure that the request originates on the host.</p>
<p>For the HTTP signature:</p> <pre>msg="MP3 GET in HTTP"</pre> <p>For the FTP signature:</p> <pre>msg="MP3 GET in FTP"</pre>	<p>Displays the name for the signature when the signature is triggered. The name appears in the Security Log. Use a descriptive string so that you can identify the triggered signature in the log.</p>
<p>For the HTTP signature:</p> <pre>regexpcntent="[Gg] [Ee] [Tt] .*[Mm] [Pp] 3 .*"</pre> <p>For the FTP signature:</p> <pre>regexpcntent="[Rr] [Ee] [Tt] [Rr] .*[Mm] [Pp] 3\x0d\x0a"</pre>	<p>Matches this string in the HTTP traffic or the FTP traffic with the payload in the TCP packets. To reduce false positives, use this argument carefully.</p> <p>The string matches the ASCII text of the TCP packet, which is "GET [.*].mp3[CR][LF]" for the HTTP signature and "RETR [.*].mp3[CR][LF]" for the FTP signature.</p> <p>The string is written so that the text can be case-insensitive.</p>

[Regular expressions in custom IPS signature content and application control rules](#)

## Memory Exploit Mitigation Settings

Use these tabs to test the Memory Exploit Mitigation policy before you apply it to the client computers, or to troubleshoot. To protect an application against an exploit, Memory Exploit Mitigation (MEM) typically either terminates the application that the exploit attacks or blocks the exploit without terminating the application. Occasionally, a mitigation technique can cause an unintended conflict with an application on the client computer. For example, the client computer may block or terminate a process that is not an exploit, which is a false positive.

- **Enable Memory Exploit Mitigation**

Disables Memory Exploit Mitigation in its entirety. Disable Memory Exploit Mitigation as a last resort to troubleshoot an application that terminated unexpectedly on the client computer. If the application then runs, reenables this option and continue to troubleshoot based on the specific mitigation technique first, and second, on the application. Re-enable Memory Exploit Mitigation when you are finished troubleshooting.

[Application Rules tab](#)

**Table 521: Mitigation Techniques tab**

Setting	Description
<b>Set the protection action for all techniques to log only</b>	<p>Disables protection for all mitigation techniques but logs any events that a technique takes on an application. This action overrides the default action that you use for each specific technique. Use this setting when you are not sure which technique is causing a conflict with the application that the client terminated.</p> <p>The following techniques ignore this setting, and continue to use their current actions:</p> <ul style="list-style-type: none"> <li>• ForceDEP</li> <li>• ForceASLR</li> <li>• EnhASLR</li> <li>• NullProt</li> </ul> <p>MEM logs the events in the <b>Network and Host Exploitation &gt; Memory Exploit Mitigation</b> log.</p>
<b>Choose a mitigation technique</b>	<p>MEM uses multiple types of techniques to handle the exploit, depending on which technique is most appropriate for the type of application. Some techniques protect multiple applications. Use this option when you know which technique terminated the application that ran on the client computer.</p> <p>For information on how each mitigation technique works, see:  <a href="#">Symantec Endpoint Protection Memory Exploit Mitigation techniques</a></p>
<b>Choose a protection action for all applications in this list</b>	<p>Overrides the default action for all the applications protected by the specific mitigation technique. Use this option in the following cases:</p> <ul style="list-style-type: none"> <li>• If you want to test a technique in audit mode before rolling it out to all clients</li> <li>• If you have determined that coverage caused unintended behavior side-effects that are a false positive, and coverage must be disabled.</li> <li>• <b>Default (Yes) and Yes</b> Protects the client by terminating the application or blocking the exploit, and logging the event in the <b>Network and Host Exploitation &gt; Memory Exploit Mitigation</b> log.</li> <li>• <b>No</b> Takes no action on the application or exploit; it neither protects the client or logs the event. Use this option only after you determine that the mitigation technique has a conflict with the application or the supposed exploit is a false positive. Notify Symantec Security Response of the conflict. After Symantec resolves the issue, turn the protection back on by changing the action to <b>Yes</b>.</li> <li>• <b>Log only</b> Takes no action on the application or exploit but logs the event. It does not protect the client. Use this option to test that a mitigation technique does not cause side-effects due to an unexpected application conflict with MEM. Symantec Endpoint Protection logs all events in the <b>Network and Host Exploitation &gt; Memory Exploit Mitigation</b> log. After Symantec resolves the issue, turn the action to <b>Yes</b>.</li> </ul>
<b>Choose override action for a particular application is protected by &lt;technique&gt;</b>	<p>Change the default action in the following cases:</p> <ul style="list-style-type: none"> <li>• You want to test a mitigation technique for all applications in log only mode before you apply the policy to the client computers.</li> <li>• You have determined that coverage causes unintended behavior side-effects that are a false positive and must be disabled.</li> </ul>

**Table 522: Application Rules tab**

Setting	Description
<b>Application Rules</b>	Use this tab to choose which applications that MEM protects or does not protect, regardless of the technique. Use this option if you do not know which technique caused the application to terminate. If you disable the protection, Memory Exploit Mitigation takes no action on the application that runs on the client. It neither protects the action, or logs an event. You must run LiveUpdate at least once for the application list to appear in the list. <a href="#">Checking that Symantec Endpoint Protection Manager has the latest content</a>

## Memory Exploit Mitigation

Memory Exploit Mitigation stops attacks on commonly used software that the vendor has not patched on Windows computers. Memory Exploit Mitigation uses various mitigation techniques to detect the exploit attempt. Each technique then either blocks the exploit or terminates the application that the exploit threatens.

## Host Integrity Policy

### Requirements

You must add requirements to the policy for the Host Integrity check to be effective. If you do not add any requirements, the client computer runs a compliance check but does not check any requirements.

You can add predefined requirements, custom requirements, or requirements from templates.

After you add a requirement, it is enabled.

When you move a requirement up or down in the list, you determine the order in which the requirements are executed. The position can be important when you download software that requires a restart after installation. You should set the order so that the requirements that require a restart for remediation are performed last.

**Table 523: New requirement settings**

Setting	Description
<b>Always do Host Integrity checking</b>	When you finish your testing phase, turn on Host Integrity checking with this choice.
<b>Only do Host Integrity checking when connected to the management server</b>	Checks the Host Integrity requirements on the clients that are connected to the management server.
<b>Never do Host Integrity checking</b>	Turns off the Host Integrity check while you finish fine-tuning your requirements. You might use the method do troubleshoot individual requirements.

## Add Requirement

Add a new Host Integrity requirement to run on a Windows client.

You must first add and enable a requirement to the Host Integrity policy for the Host Integrity check to be effective.

## Advanced Settings

Use this dialog box to configure options for the Host Integrity check, remediation, and notifications.

**Table 524: Host Integrity advanced settings**

Setting	Description
<b>Host Integrity Checking Options</b>	<p>Specifies the following Host Integrity check options:</p> <ul style="list-style-type: none"> <li>• <b>Check Host Integrity every</b> Specifies how often the Host Integrity check runs on the client computer. Type an integer from 1 to 24855.</li> <li>• <b>Keep results of check for</b> Sets the duration that the client retains the results of the previous Host Integrity check. The client maintains the result even if the user takes an action that would normally result in a new Host Integrity check. For example, a client may download new software or change a location, either of which can increase their security risk.</li> <li>• <b>Continue to check requirements after one fails</b> The client checks the Host Integrity requirements in the order that is specified in the Host Integrity policy. Therefore, you may want to allow the client to continue checking the requirements even if one requirement fails. Otherwise, the client stops the Host Integrity check until the failed requirement is remediated and passes. You can apply the <b>Allow the Host Integrity check to pass even if this requirement fails</b> option for each requirement type separately. For example, if you add an antivirus requirement and a firewall requirement, the Host Integrity check still passes even if one of the requirements fails.</li> </ul>
<b>Remediation Dialog Options</b>	<p><b>Gives the client users the option to cancel Host Integrity checking if the first check fails. Use this option in the following situations:</b></p> <ul style="list-style-type: none"> <li>• If you want to troubleshoot or test a new Host Integrity policy.</li> <li>• If you want to give the users the option to continue working while their system remediates.</li> <li>• <b>Allow the user to cancel remediation for</b> Specifies the minimum time and maximum time users can postpone a remediation action.</li> <li>• <b>Number of times the user is allowed to cancel remediation</b> Enables the client user to postpone a remediation file from being downloaded and installed. You may want to enable this option if the remediation interrupts the user's work. Users can cancel remediation an unlimited number of times.</li> <li>• <b>Set Additional Text</b> You can provide instructions on how to remediate for client users when the client fails a requirement. <a href="#">Setting up remediation for a predefined Host Integrity requirement</a></li> </ul>
<b>Notifications</b>	<ul style="list-style-type: none"> <li>• <b>Show verbose Host Integrity Logging</b> Displays the information about the result of a Host Integrity check. That information appears in the client's Security log, in the lower right-hand pane of the log. The detailed information includes the conditions that the requirement checks for, such as a particular registry key. On the management server, to view the information, click <b>Monitors &gt; Logs &gt; Compliance &gt; Client Host Integrity</b>.</li> <li>• <b>Display a notification message when a Host Integrity check fails</b> You can display a notification to let users know that the client computer did not pass a Host Integrity check.</li> <li>• <b>Display a notification message when a Host Integrity check passes after previously failing</b> If the Host Integrity check fails and the user remediates, the user may not realize that the Host Integrity check ran again and then succeeded. You can display a notification that informs the user if the Host Integrity check passes after a previous failure. In addition to the notification, Symantec Endpoint Protection makes an entry on the management server, in <b>Monitors &gt; Logs &gt; Compliance &gt; Client Host Integrity</b>. The notification also appears in the Security log on the client.</li> </ul>

## Custom requirement: Select a condition

Use this panel to add the logic to the custom requirement.

**Table 525: Keywords for a custom requirement script**

Keyword	Description
<b>Insert statements below</b>	Enables you to add an <b>IF..THEN</b> statement, function, return value, or comment. If you add an <b>IF..THEN</b> statement, you then add a condition in the right-hand field.
<b>IF</b>	Specifies a condition that the requirement must check for on the client computer. For example, you can check for the presence or absence of antivirus software.  <b>Note:</b> You cannot have an empty <b>IF</b> node. If you need to remove the <b>IF</b> statement, right-click the node and then click <b>Delete</b> .
<b>THEN</b>	If the condition introduced by the <b>IF</b> statement is met or not met, you can specify an action to take. For example, you can download a file, run a program, set a registry value, and so on.
<b>END IF</b>	Every <b>IF..THEN</b> statement ends with <b>END IF</b> . After the <b>IF..THEN</b> statements execute, the statement following <b>END IF</b> is executed To add an <b>IF..THEN</b> statement at the same level as an existing one, select <b>END IF</b> . To add a nested <b>IF..THEN</b> statement, select the line under which you want to add it.
<b>TOGGLE NOT</b>	Checks for the absence of a condition. Right-click the condition, and then click <b>Toggle NOT</b> .
<b>ELSE</b>	Specifies the actions to be taken whenever the specified conditions are evaluated as being <i>false</i> .
<b>Pass or Return</b>	Specifies whether the requirement fails or passes the Host Integrity check.
<b>Comment</b>	Enables you to describe what the script does.

[Writing a customized requirement script](#)

## Custom requirement

Use this panel to build a custom requirement for Host Integrity.

**Table 526: Keywords for a custom requirement script**

Keyword	Description
<b>Insert statements below</b>	Enables you to add an <b>IF..THEN</b> statement, function, return value, or comment. If you add an <b>IF..THEN</b> statement, you then add a condition in the right-hand field.
<b>IF</b>	Specifies a condition that the requirement must check for on the client computer. For example, you can check for the presence or absence of antivirus software.  <b>Note:</b> You cannot have an empty <b>IF</b> node. If you need to remove the <b>IF</b> statement, right-click the node and then click <b>Delete</b> .
<b>THEN</b>	If the condition introduced by the <b>IF</b> statement is met or not met, you can specify an action to take. For example, you can download a file, run a program, set a registry value, and so on.
<b>END IF</b>	Every <b>IF..THEN</b> statement ends with <b>END IF</b> . After the <b>IF..THEN</b> statements execute, the statement following <b>END IF</b> is executed To add an <b>IF..THEN</b> statement at the same level as an existing one, select <b>END IF</b> . To add a nested <b>IF..THEN</b> statement, select the line under which you want to add it.
<b>TOGGLE NOT</b>	Checks for the absence of a condition. Right-click the condition, and then click <b>Toggle NOT</b> .
<b>ELSE</b>	Specifies the actions to be taken whenever the specified conditions are evaluated as being <i>false</i> .
<b>Pass or Return</b>	Specifies whether the requirement fails or passes the Host Integrity check.
<b>Comment</b>	Enables you to describe what the script does.

[Writing a customized requirement script](#)

## Custom Requirement: Customized Requirement Script

Use `Pass` if you want the requirement to pass as a result of the **IF..THEN** condition.

Use `Fail` if you want the requirement to fail as a result of the **IF..THEN** condition.

## Add Requirement: Antivirus requirement

Checks that an antivirus application is installed and running on the client.

**Table 527: Antivirus requirements**

Setting	Description
<b>Antivirus application that must be installed and running</b>	Checks for the specified application on the client computer. If you click <b>Any antivirus product</b> , any of the applications on the drop-down list fulfill the requirement. You do not have options to set up remediation. If you click a specific antivirus application and it is not installed, you can set remediation options to download and install the file.
<b>Install antivirus if it has not been installed on client</b>	Sets up remediation so that the client downloads and installs the missing application. <ul style="list-style-type: none"><li>• <b>Install antivirus if it has not been installed on the client.</b> Checks whether or not the application is installed on the client computer.</li><li>• <b>Download the installation package.</b> If the application is not installed on the client computer, enables the following options to download and install the application:<ul style="list-style-type: none"><li>– <b>Download URL</b> Specifies the location from which the installation file can be downloaded.</li><li>– <b>Execute the command</b> Specifies whether the client user runs the installation or the installation runs automatically. To let the client user run the installation, leave the text box blank. To let the installation run automatically, you can type: <code>%F%</code>. <a href="#">About specifying the file location and execute command for remediation</a></li></ul></li></ul>
<b>Start antivirus if it is not running on the client</b>	Starts the application after it is installed. In the <b>Execute the command</b> field, type the command that starts the application.
<b>Antivirus Signature File Checking</b>	<b>Checks that the signature file is up to date.</b> <ul style="list-style-type: none"><li>• <b>Specify the oldest age of the signature file</b> Lets you select a relative time value for the signature file age.</li><li>• <b>Check the signature file date</b> Lets you select a specific date and time when the signature file was last modified.</li><li>• <b>If not, update the signature file</b> Lets you download and update the signature file if it is out of date. Specify the location from which to download the file. <b>Note:</b> The file's last-modified date determines the signature file age.</li><li>• <b>Execute the command</b> Type the following: <code>%F%</code>.</li></ul>
<b>Check Antivirus Infected Status</b>	Checks that a Symantec Endpoint Protection antivirus scan has been run and that the client computer is not infected. Only Windows computers that run Symantec Endpoint Protection can use this condition.
<b>Specify wait time before attempting the download again if the download fails</b>	Specifies a time to wait before the client tries to download and start the application again.

Setting	Description
<b>Allow the user to cancel the download for Host Integrity remediation</b>	Enables the user to cancel remediation. You may want to enable users to cancel or delay remediation to avoid disruption to their work. If you disable this option, the user is notified that a download is in progress. However, the user is not given the option to cancel or postpone the remediation.
<b>Allow the Host Integrity check to pass even if this requirement fails</b>	Enables the user to connect to the network even though the client computer fails this Host Integrity requirement. The failed requirement is logged in the client's Security log.

## Add Requirement: Antispyware requirement

Checks that an antispyware application is installed and running on the client.

**Table 528: Antispyware requirements**

Setting	Description
<b>Antispyware application that must be installed and running</b>	Checks for the specified application on the client computer. If you click <b>Any antispyware product</b> , any of the applications in the drop-down list fulfill the requirement. You do not have options to set remediation.
<b>Install antispyware if it has not been installed on client</b>	Sets up remediation so that the client downloads and installs the missing application. <ul style="list-style-type: none"> <li>• <b>Install antispyware if it has not been installed on the client.</b> Checks whether or not the application is installed on the client computer.</li> <li>• <b>Download the installation package.</b> If the application is not installed on the client computer, enables the following options to download and install the application: <ul style="list-style-type: none"> <li>– <b>Download URL</b> Specifies the location from which the installation file can be downloaded.</li> <li>– <b>Execute the command</b> Specifies whether the client user runs the installation or the installation runs automatically. To let the client user run the installation, leave the text box blank. To let the installation run automatically, you can type: %F%. <a href="#">About specifying the file location and execute command for remediation</a></li> </ul> </li> </ul>
<b>Start antispyware if it is not running on the client</b>	Starts the application after it is installed. In the <b>Execute the command</b> field, type the command that starts the application.
<b>Antispyware Signature File Checking</b>	<b>Checks that the signature file is up to date.</b> <ul style="list-style-type: none"> <li>• <b>Specify the oldest age of the signature file</b> Lets you select a relative time value for the signature file age.</li> <li>• <b>Check the signature file date</b> Lets you select a specific date and time when the signature file was last modified.</li> <li>• <b>If not, update the signature file</b> Lets you download and update the signature file if it is out of date. Specify the location from which to download the file. <b>Note:</b> The file's last-modified date determines the signature file age.</li> <li>• <b>Execute the command</b> Type the following: %F%.</li> </ul>
<b>Specify wait time before attempting the download again if the download fails</b>	Specifies a time to wait before the client tries to download and start the application again.

Setting	Description
<b>Allow the user to cancel the download for Host Integrity remediation</b>	Enables the user to cancel remediation. You may want to enable users to cancel or delay remediation to avoid disruption to their work. If you disable this option, the user is notified that a download is in progress. However, the user is not given the option to cancel or postpone the remediation.
<b>Allow the Host Integrity check to pass even if this requirement fails</b>	Enables the user to connect to the network even though the client computer fails this Host Integrity requirement. The failed requirement is logged in the client's Security log.

## Add Requirement: Patch

Adds a requirement to check that the client computer has a specific patch for the client computer's operating system. If you have one patch that applies to multiple operating systems, you can include them all in one requirement.

### WARNING

Review your selections carefully. If you select an operating system that does not match the patch, the requirement fails.

**Table 529: Patch requirements**

Setting	Description
<b>Patch Name</b> that must be installed	Describes the patch that must be installed on the client computer. Type the patch name, such as KB12345. You can type only numbers and letters in this field.
<b>Apply the patch on these operating systems</b>	Specifies the operating systems for which the patch must be installed. You can choose one or more, but the patch name must apply to all selected operating systems.
<b>Install the patch if it has not been installed on the client</b>	Installs a new patch on the client computer from the management server. You can uncheck this check box if you want to use the Microsoft management software to install the patch. However, if you uncheck this option and the required patch is not installed on the client computer, the Host Integrity check fails on this requirement. <ul style="list-style-type: none"> <li>• <b>Install the patch if it has not been installed on the client.</b> Checks whether or not the application is installed on the client computer.</li> <li>• <b>Download the installation package.</b> If the application is not installed on the client computer, enables the following options to download and install the application: <ul style="list-style-type: none"> <li>– <b>Download URL</b> Specifies the location from which the installation file can be downloaded.</li> <li>– <b>Execute the command</b> Specifies whether the client user runs the installation or the installation runs automatically. To let the client user run the installation, leave the text box blank. To let the installation run automatically, you can type: %F%. <a href="#">About specifying the file location and execute command for remediation</a></li> </ul> </li> </ul>
<b>Run the program</b>	Specifies whether the user needs to be logged on to the client for the program to run. <ul style="list-style-type: none"> <li>• <b>in system context</b> The user does not have to be logged on for the program to run.</li> <li>• <b>in logged-in user context</b> The user must be logged on to the client for the program to run. The execute command line must include the full path name.</li> </ul>
<b>Specify wait time before attempting the download again if the download fails</b>	Specifies a time to wait before the client tries to download and start the application again.



Setting	Description
<b>Allow the user to cancel the download for Host Integrity remediation</b>	Enables the user to cancel remediation. You may want to enable users to cancel or delay remediation to avoid disruption to their work. If you disable this option, the user is notified that a download is in progress. However, the user is not given the option to cancel or postpone the remediation.
<b>Allow the Host Integrity check to pass even if this requirement fails</b>	Enables the user to connect to the network even though the client computer fails this Host Integrity requirement. The failed requirement is logged in the client's Security log.

## Add Requirement: Service pack

Adds a requirement to check that the client computer has a specific service pack for the client computer's operating system.

If there is one service pack that applies to multiple versions of the operating system, you can specify them all in one requirement. You can use Select All and Clear All to make it easier to work with the list.

This requirement checks the registry or uses Windows APIs to see if the specified service pack is installed.

### WARNING

Review your selections carefully. If you select an operating system that does not match the service pack number, the requirement fails.

**Table 530: Service pack requirements**

Setting	Description
<b>Specify the minimum Service Pack Number which must be installed on the following operating systems</b>	Specifies the number of the service pack. An example is 1. The number is limited to a single character. You can type only numbers from 1 to 9. Make sure that the operating systems that you check match the service pack number that you typed.
<b>Install the service pack if it has not been installed on the client</b>	<p>Installed the specified service pack on the client computer</p> <ul style="list-style-type: none"> <li>• <b>Install the service pack if it has not been installed on the client.</b> Checks whether or not the application is installed on the client computer.</li> <li>• <b>Download the installation package.</b> If the application is not installed on the client computer, enables the following options to download and install the application: <ul style="list-style-type: none"> <li>– <b>Download URL</b> Specifies the location from which the installation file can be downloaded.</li> <li>– <b>Execute the command</b> Specifies whether the client user runs the installation or the installation runs automatically. To let the client user run the installation, leave the text box blank. To let the installation run automatically, you can type: %F%. <a href="#">About specifying the file location and execute command for remediation</a></li> </ul> </li> </ul>
<b>Specify wait time before attempting the download again if the download fails</b>	Specifies a time to wait before the client tries to download and start the application again.
<b>Allow the user to cancel the download for Host Integrity remediation</b>	Enables the user to cancel remediation. You may want to enable users to cancel or delay remediation to avoid disruption to their work. If you disable this option, the user is notified that a download is in progress. However, the user is not given the option to cancel or postpone the remediation.
<b>Allow the Host Integrity check to pass even if this requirement fails</b>	Enables the user to connect to the network even though the client computer fails this Host Integrity requirement. The failed requirement is logged in the client's Security log.

## Add Requirement: Firewall requirement

Checks that a firewall application is installed and running on the client.

Table 531: Firewall requirements

Setting	Description
Firewall application that must be installed and running	Checks for the specified firewall application on the client computer If you click <b>Any firewall product</b> , any application on the drop-down list fulfills the requirement. You do not have options to set remediation.
Install the firewall if it has not been installed on the client	Sets up remediation so that the client downloads and installs the missing application. <ul style="list-style-type: none"><li>• <b>Install the firewall if it has not been installed on the client.</b> Checks whether or not the application is installed on the client computer.</li><li>• <b>Download the installation package.</b> If the application is not installed on the client computer, enables the following options to download and install the application:<ul style="list-style-type: none"><li>– <b>Download URL</b> Specifies the location from which the installation file can be downloaded.</li><li>– <b>Execute the command</b> Specifies whether the client user runs the installation or the installation runs automatically. To let the client user run the installation, leave the text box blank. To let the installation run automatically, you can type: %F%. <a href="#">About specifying the file location and execute command for remediation</a></li></ul></li></ul>
Start the firewall if it is not running on the client	Starts the application after it is installed. In the <b>Execute the command</b> field, type the command that starts the application.
Specify wait time before attempting the download again if the download fails	Specifies a time to wait before the client tries to download and start the application again.
Allow the user to cancel download for Host Integrity remediation	Enables the user to cancel remediation. You may want to enable users to cancel or delay remediation to avoid disruption to their work. If you disable this option, the user is notified that a download is in progress. However, the user is not given the option to cancel or postpone the remediation.
Allow the Host Integrity check to pass even if this requirement fails	Enables the user to connect to the network even though the client computer fails this Host Integrity requirement. The failed requirement is logged in the client's Security log.

---

## About specifying the file location and execute command for remediation

To set up remediation so that the client downloads and installs the missing application, you specify a download location and run command.

<b>Download URL</b>	<p>Specifies the location from which the installation file can be downloaded.</p> <p>When you specify the location of the installation file or package to be downloaded, you can use any of the following formats:</p> <ul style="list-style-type: none"><li>• <b>UNC</b> \\servername\sharename\dirname\filename UNC restore does not work if Network Neighborhood browsing is disabled on the target client. Be certain that Network Neighborhood browsing has not been disabled if you use UNC paths for remediation.</li><li>• <b>FTP</b> FTP://ftp.ourftp.ourcompany.com/folder/filename</li><li>• <b>HTTP</b> HTTP://www.ourwww.ourcompany.com/folder/filename</li></ul> <p>Installation packages or files in Windows are always downloaded to the temporary directory. Any relative path refers to this directory. The temporary directory is defined in the TMP environment variable if it exists, or in the TEMP environment variable if that exists. The default directory is in the Windows directory.</p> <p>For file execution, the current working directory is always set to the Windows temporary directory. Environment variables are substituted before execution. The Windows directory path replaces the command %windir%.</p>
<b>Execute the command</b>	<p>Specifies whether the client user runs the installation or the installation runs automatically.</p> <ul style="list-style-type: none"><li>• To let the client user run the installation, leave the text box blank.</li><li>• To let the installation run automatically, you can type: %F%.</li></ul> <p>If you do not select to download an installation package, you can still specify a command for the client to execute. The client tries to install the missing application. You specify the command by giving the full path name of the executable file. FTP and UNC paths are supported. If you are familiar with variable representation, you can modify the command entry. Also, if you need to allow another application to be used to execute the program that is downloaded, you can modify the command entry. The following is an example of proper syntax:</p> <pre>C:\program files\WinZIP\winzip.exe -a -s %1 -r c:\temp</pre>

[Setting up remediation for a predefined Host Integrity requirement](#)

### Antivirus: Antivirus is installed

Checks that the selected antivirus application is installed on the client computer.

### Antivirus: Antivirus is running

Checks that the selected antivirus application runs on the client computer.

### Antivirus: Antivirus signature file is up-to-date

Checks that the antivirus signature file is up to date.

**Table 532: Antivirus signature file is up-to-date**

Setting	Description
<b>Antivirus name</b>	Specifies the name of the antivirus software package.
<b>Check if the age in days of the signature file is less than</b>	Checks whether the signature file has been uploaded to the client computer within the number of specified days. The default number of days is seven, but there is no limit.
<b>Check the date of the signature file</b>	Checks whether the signature file date is older, more recent, or equal to the specified day and time. The default date is the current day and the default time is 00:00.

## **Antispyware: Antispyware is installed**

Checks that the selected antispyware application is installed on the client computer.

## **Antispyware: Antispyware is running**

Checks that the selected antispyware application runs on the client computer.

## **Antispyware: Antispyware signature file is up-to-date**

Checks that the client's antispyware signature file is up to date.

**Table 533: Antispyware signature file is up-to-date settings**

Setting	Description
<b>Antispyware name</b>	Specifies the name of the antispyware software package.
<b>Check if the age in days of the signature file is less than</b>	Checks whether the signature file has been uploaded to the client computer within the number of specified days. The default number of days is seven, but there is no limit.
<b>Check the date of the signature file</b>	Checks whether the signature file date is older, more recent, or equal to the specified day and time. The default date is the current day and the default time is 00:00.

## **Antivirus: Check not infected**

Checks that a Symantec Endpoint Protection antivirus scan has been run and the client computer is not infected. Only Windows computers that run Symantec Endpoint Protection can use this condition.

## **Firewall: Firewall is installed**

Checks whether the selected firewall application is installed on the client computer.

## **Firewall: Firewall is running**

Checks that the selected firewall application runs on the client computer.

## **Patch: Compare current service pack with specified version**

Compares the service pack number you specify with the service pack number on the client computer. You can specify equal to, not equal to, less than, or greater than.

---

## Patch: Patch is installed

Checks that the patch you specify is installed on the client computer.

Specify the patch name, such as KB12345.

### NOTE

You must type only letters and numbers in this field.

## File: Compare file age to

Checks how many days or weeks have passed since the file was last saved. This information can help you decide whether the file version on the client computer is up to date.

## File: Compare file date to

Checks the date of a file on the client computer. The condition determines whether the date is later than, earlier than, a different date than, or equal to the specified date and time. This information may add to a decision on whether the version on the client computer is up to date.

The maximum number of characters you can type is 255 characters.

## File: Compare file size to

Check the size of a file that runs on the client computer. The results determine whether the size is equal to, not equal to, less than, or greater than a certain size. This information may add to a decision on whether the version on the client computer is up to date.

## File: Compare file version to

Checks that the file version on the client computer is the same as the version you specify. This information may add to a decision on whether the version on the client computer is up to date.

You can compare by specifying a system environment variable. You can also specify the registry values that are equal to, not equal to, less than, or greater than the number you compare.

## File: File download complete

Checks to confirm that the file download that you specified has completed. Once the download has completed, you can take the next step in your custom requirement script.

**Table 534: File download complete settings**

Setting	Description
<b>File URL</b>	Specifies the URL of the file to be downloaded.
<b>Target folder</b>	Specifies the folder on the client computer to which you want the file to be saved.
<b>Authentication required for HTTP only</b>	Specifies the user name and password that the user needs to download the file. If you want users to download the file from an FTP or UNC file share, you must set up the target site to allow anonymous access. If you want extra security, use this option and set up an HTTP server to download the file. You can set up the user name and password in the user interface of the HTTP server.

Setting	Description
<b>Show the download process dialog</b>	Displays the download process dialog box on the client computer. You may want to allow the users to cancel the Host Integrity check for this requirement if the file download interrupts their work.

## File: File exists

Checks that a certain file exists on the specified path on the client. If the file does not exist in the location you specify, you can specify that the client download a copy.

You can specify the file by path, system environment variable, or registry value.

## File: File fingerprint equals

Checks that an application file on the client has the specified file fingerprint. A file fingerprint is a checksum of an executable or DLL on a client computer.

You can find the path, the file name, and the file fingerprint of an application from the **Search for Applications** dialog box. To access this feature, click **Policies > Search for Applications**.

[Creating a file fingerprint list with checksum.exe](#)

## Registry: Registry key exists

Specify a registry key name to check whether it exists.

### NOTE

Do not use shortened registry keys, such as `HKLM`. Always spell out registry keys. In this example, use `HKEY_LOCAL_MACHINE` instead of `HKLM`.

**Table 535: Registry key exists settings**

Setting	Description
<b>Registry key</b>	Checks whether the following registry key exists.

## Registry: Registry value exists

Specify a registry key value to check whether it has the specified value name. The form of the value can be DWORD, string, or binary.

### NOTE

Do not use shortened registry keys, such as `HKLM`. Always spell out registry keys. In this example, use `HKEY_LOCAL_MACHINE` instead of `HKLM`.

**Table 536: Registry value exists settings**

Setting	Description
<b>Registry key</b>	Specifies the registry key that contains the value name to be checked.
<b>Value name</b>	Checks whether the value name exists.

---

## Registry: Registry value equals

Specify a registry key name and a value name and data to compare the value against. The form of the value can be DWORD, string, or binary.

### NOTE

Do not use shortened registry keys, such as `HKLM`. Always spell out registry keys. In this example, use `HKEY_LOCAL_MACHINE` instead of `HKLM`.

**Table 537: Set registry value settings**

Setting	Description
Registry key	Specifies the registry key that contains the value name and type to be checked.
Value name	Specifies the value name to be checked.
Data to Compare Against	Checks for the values for each type of data that is specified in the list that appears.

## Registry: Set registry value

Sets a registry entry to a specific value. The Set registry value function creates the value if it does not already exist. You can specify the registry key name and your desired value.

### NOTE

Do not use shortened registry keys, such as `HKLM`. Always spell out registry keys. In this example, use `HKEY_LOCAL_MACHINE` instead of `HKLM`.

**Table 538: Set registry value settings**

Setting	Description
Registry key	Specifies the registry key that contains the value name and type to be checked.
Value name	Specifies the value name to be used.
Specify Type and Data	Checks for the value type and content that is specified in the list that appears.

## Registry: Set registry value successful

Checks the registry to ensure that the registry value you set in Set registry value was set successfully.

### NOTE

Do not use shortened registry keys, such as `HKLM`. Always spell out registry keys. In this example, use `HKEY_LOCAL_MACHINE` instead of `HKLM`.

**Table 539: Set registry value settings**

Setting	Description
Registry key	Specifies the registry key that contains the value name and type to be checked.
Value name	Specifies the value name to be checked.
Specify Type and Data	Checks for the value type and content that is specified in the list that appears.

---

## Registry: Increment registry DWORD value

Lets you add registry DWORD value settings. This selection lets you perform counts, such as allowing an unpatched computer to meet the requirement no more than n times. Creates the key that contains the DWORD value if it does not exist.

### NOTE

Do not use shortened registry keys, such as `HKLM`. Always spell out registry keys. In this example, use `HKEY_LOCAL_MACHINE` instead of `HKLM`.

**Table 540: Increment registry DWORD value settings**

Setting	Description
Registry key	Specifies the registry key that contains the DWORD value name to be checked.
Value name	Checks for the DWORD value name, such as <code>0x000001</code> .

## Utility: Check timestamp

Compares the current time with a value that has been stored in the registry using the Set timestamp utility. You use the Check Timestamp condition to find out whether a specified amount of time has passed since that timestamp was created. For example, if the Host Integrity check runs every 2 minutes, you can specify an action to occur at a longer interval. In this case, the stored time value is removed. If no timestamp has been created with Set timestamp, this function returns True.

## Utility: Message dialog return value equals true

Configures a message box that appears on the client computer. You can add text and various buttons and icons. If the user clicks the **OK** or **Yes** buttons, the message box returns a value of True. If the user clicks the **No** or **Cancel** buttons, the message box returns a value of False. This dialog lets you specify a condition that looks for either a True value or a False value. You can also specify a wait time after which a response of **OK** is automatically entered.

## Utility: Operating system is

Specify the operating system that you want the client computer to run. You can choose a single operating system or multiple operating systems. One reason to use this function is to verify that a patch you apply to the client works with the specified operating system.

## Utility: Operating system language is

Detects the language version of the client's operating system. You can choose a single language or multiple languages. You can use this condition to guide your choice of patches and updates to install, if they are language-specific.

## Utility: Process is running

Checks whether a specific process that you name is running on the client computer. This condition enables you to avoid problems with any processes that might conflict with your script. It also enables you to leverage any processes that you want to be certain are running on the client computer.



---

## Utility: Service is running

Checks that a specific service runs on the client computer. This condition lets you avoid conflicts between a service and your script. It also lets you leverage any services that you want to be certain are running on the client.

## File: Download a file

Downloads a file onto the client computer. You can specify the conditions so that the client downloads the file from a URL to a destination folder on the client. You can follow this function with the Run a program function.

**Table 541: Download a file settings**

Setting	Description
<b>File URL</b>	Specifies the URL from where the file is downloaded.
<b>Target folder</b>	Specifies the folder on the client computer to which you want the file to be saved.
<b>Authentication required for HTTP only</b>	Specifies the user name and password that the user needs to download the file. If you want users to download the file from an FTP or UNC file share, you must enable the target server to allow anonymous access. If you want extra security, use this option and set up an HTTP server to download the file. You can set up the user name and password in the user interface of the HTTP server.
<b>Show the download process dialog</b>	Displays the download process dialog box on the client computer. You may want to allow the users to cancel the Host Integrity check for this requirement if the file download interrupts their work.

## Utility: Log message

Displays a log message on the client's computer. You can use this function to inform the user of the results of checks that you have run. The results also appear in the client's Security log and are informational only.

For a message that requires the user to respond, use the Show message dialog utility.

[Utility: Show message dialog](#)

## Utility: Run a program

Specifies a program that runs on the client computer. This utility is frequently used with the Download a file utility.

**Table 542: Run a program settings**

Setting	Description
<b>Specify the command that runs the application</b>	Executes the command you type in this dialog box on the client computer, including the full path. You can include environment variables.
<b>Run the Program</b>	<p>Specifies whether the user needs to be logged on to the client for the program to run.</p> <ul style="list-style-type: none"><li>• <b>in system context</b> The user does not have to be logged on for the program to run. Use this option if you want the program to run on the client immediately, for security purposes. For example, the client may need to have an antivirus program installed.</li><li>• <b>in logged-on user context</b> The user must be logged on to the client for the program to run.</li></ul>

Setting	Description
<b>Specify the Maximum Waiting Time for the Program to Complete</b>	Specifies the maximum waiting time for the program to complete. If the function times out, the execution of the program terminates.
<b>Show a new process window</b>	Shows a process window where the user can watch the program run.

## Utility: Run a script

Specifies a script that should run on the client computer.

**Table 543: Run a script settings**

Setting	Description
<b>File name</b>	Specifies a file name for the script.
<b>Script content</b>	Specifies the script content.
<b>Execute the command</b>	Specifies the command to execute the script.
<b>Specify the Maximum Waiting Time for the Program to Complete</b>	Specifies the maximum waiting time it takes the client computer to finish running the script before the script terminates.
<b>Delete the temporary file after execution is completed or terminated</b>	Removes the temporary file after the script runs or is terminated, if a temporary file is created.
<b>Show a new process window</b>	Displays a window where the user can watch the script run.

## Utility: Set timestamp

Names a timestamp that is stored on the client computer's registry. You use the Set timestamp utility with the Check timestamp utility. You use the Check timestamp utility to check whether a specified amount of time has passed since the named timestamp was created. You can use the two utilities to check when certain actions have occurred since the named timestamp was set.

Type a name of up to 255 characters.

## Utility: Show message dialog

Displays a message on the client computer, and waits for the user's response.

To display a message that is informational only and requires no user action, use the function for the Log message utility.

In the **Text of the message box** field, the special characters >, =, or the tab do not appear in the message box on the client.

## Utility: Wait

You can use this utility when a script or a program runs, and you want the script to resume after a specified amount of time.

## Miscellaneous: Virtual Images

You must create the baseline images that you want to exclude with the Virtual Image Exclusion tool.

**Table 544: Virtual Images**

Option	Description
<b>Enable Virtual Image Exception for Auto-Protect</b>	Symantec Endpoint Protection does not scan the files that Virtual Image Exception has marked for exception when it performs an Auto-Protect scan. This option is disabled by default.
<b>Enable Virtual Image Exception for Administrator-Defined Scans</b>	Symantec Endpoint Protection does not scan the files that Virtual Image Exception has set for exception when it performs manual scans or scheduled scans. This option is disabled by default.

**NOTE**

Symantec supports the use of the Virtual Image Exception feature only in virtual desktop infrastructures.

**Miscellaneous: Shared Insight Cache**

You can use a Shared Insight Cache that clients access over a network. Clients use Shared Insight Cache for scheduled scans and manual scans.

As of 14, a Shared Insight Cache that is integrated with VMware vShield is no longer supported.

**Table 545: Shared Insight Cache options**

Option	Description
<b>Shared Insight Cache using Network</b>	Enables the Shared Insight Cache to communicate with Symantec Endpoint Protection clients through the network.
<b>Require SSL</b>	<p>Enables Shared Insight Cache to use SSL authentication. By default, Shared Insight Cache uses no authentication and no SSL.</p> <p>To use SSL authentication, you must enable SSL as a part of the Shared Insight Cache server settings in the configuration file.</p> <p><a href="#">Customizing Shared Insight Cache settings</a></p> <p>If you enable SSL, you must also set up your clients to communicate with Shared Insight Cache by adding the Shared Insight Cache server certificate to the trusted certificates authorities store for the local computer. Otherwise, the communication between the clients and the Shared Insight Cache fails.</p> <p>For information about how to add a server certificate, see your Active Directory documentation.</p> <p>If you changed the SharedInsightCacheService.exe.config file to set Shared Insight Cache to use Basic Authentication with SSL or Basic Authentication with no SSL, type the following information:</p> <ul style="list-style-type: none"> <li>• <b>Username</b> The authentication user name.</li> <li>• <b>Change Password</b> The authentication password. The default setting for the password is null. In other words, the password is blank. You can change a user-defined authentication password. But if you do, you must specify that authentication user name and password in Symantec Endpoint Protection Manager so that clients can communicate with Shared Insight Cache.</li> </ul>
<b>Hostname</b>	Specify the host name for the Shared Insight Cache server.
<b>Port</b>	Specify the port that Shared Insight Cache uses.

---

## Change Password

By default, network-based Shared Insight Cache does not use authentication or SSL. The default setting for the password is null (blank). If you changed the SharedInsightCacheInstallation.exe.config file to set network-based Shared Insight Cache to use Basic authentication with SSL or Basic Authentication with no SSL, then you must specify the user's password to allow access to Shared Insight Cache.

You can also change a user-defined authentication password if needed.

**Table 546:**

Option	Description
Username	If you changed the SharedInsightCacheService.exe.config file to set Shared Insight Cache to use Basic authentication with SSL or Basic Authentication with no SSL, type the authentication user name.
Change Password	If you changed the SharedInsightCacheService.exe.config file to set Shared Insight Cache to use Basic authentication with SSL or Basic Authentication with no SSL, use this option to specify and confirm the authentication password.

[About Shared Insight Cache](#)

## Private Cloud

You can specify that private servers manage Insight lookups and submissions for the current group. If you use a private Insight server, and configured that server as part of the **Site** properties, you must disable the site-wide option to use the group option here. The site-wide option takes precedence.

### NOTE

You can apply these settings to other groups from this dialog. You do not have to modify each group's policy.

**Table 547: Private cloud options**

Option	Description
Enable private servers to manage my data	Lets private servers manage the data for the current group. If you have the site-wide option for private servers enabled, the site-wide option takes precedence. Disable the site-wide option to use this group option. Go to <b>Admin &gt; Servers</b> , select the site and then under <b>Tasks</b> select <b>Edit Site Properties &gt; Private Insight Server</b> .
Use Symantec EDR servers for Insight lookups and submissions	Select this option if you use a Symantec Endpoint Detection and Response (Symantec EDR) server in your environment to collect information and perform additional analysis about threats. The Symantec EDR server handles both Insight lookups as well as submissions about detections. Symantec EDR sends both to Symantec to process.
Use a private Insight server for Insight lookups	Select this option if you want to use a private Insight server for Insight lookups for clients in the current group. The private Insight server uses a copy of the Symantec Insight database. Clients continue to send submissions about detections directly to Symantec.
Use Symantec servers when private servers are not available	Lets clients in the group send reputation queries and submissions to Symantec if the private servers are not available.

Option	Description
<b>Private Servers</b>	You can add a list of private servers to priority groups. Group 1 has priority when servers in the group are available. If no servers in priority group 1 are available, then clients use the servers in group 2, and so on. In each priority group, however, each server in the priority group has the same priority.
<b>Copy settings</b>	The private server settings apply to the current group, but you can apply the private server settings to additional groups and locations.

## Copy private server settings

Use this dialog box to copy the Private Cloud settings to additional groups and locations. The settings apply to the current group by default. You must check the group or location for the settings to become effective.

For any future changes you make to this group, you must recopy the settings to the additional groups and locations.

The icons display the following information:

- A folder icon indicates a group.
- A round icon indicates a location.
- Text that is grayed out indicates that the group or location inherits its setting from its parent group.

To select the parent group and all subgroups, right-click a parent and choose **Select All Subgroups**.

## Private Cloud: Add or Edit Private Server

Specify information about the private server that you want to add to the list.

**Table 548: Add Private Server options**

Option	Description
<b>Server URL</b>	Specifies the server URL. Select the protocol from the drop-down menu and then enter the host name.
<b>Port</b>	Specifies the port for the server in the range 1 to 65535. By default, the HTTP port is 80. By default, the HTTPS port is 443.
<b>Use this server as the private Insight server for 12.1.5 clients and earlier</b>	Any clients 12.1.5 and earlier cannot use a list of servers. You can designate this server as the single server that 12.1.5 and earlier clients use. If this server is unavailable, 12.1.5 and earlier clients cannot use Symantec servers. Reputation queries and submissions from these clients are essentially disabled.

## Cloud: Overview

This page provides an overview for the Cloud tab.

**Table 549: Cloud overview options**

Screen	Description
<b>Welcome</b>	<p>The <b>Cloud</b> tab lets you begin enrollment with the cloud console. You can also enter your enrollment token if you already have one. You get the enrollment token through Symantec Endpoint Security.</p> <p><b>Note:</b> After you enroll, if you see an alert about the connection, follow the instructions on this page:</p> <p><b>Note:</b> <a href="#">Certificate error when using a web browser to view the manager console</a></p> <p>Click <b>Troubleshooting</b> for status information, and click <b>Unenroll</b> to unenroll Symantec Endpoint Protection Manager from the cloud console.</p>
<b>Troubleshooting</b>	<p>This tab displays the following information about the active connector that is responsible for data upload and download:</p> <ul style="list-style-type: none"> <li>• <b>Installation Status</b> Displays whether the connector for cloud enrollment is installed.</li> <li>• <b>Active Connector</b> Displays the server that acts as the connector to the cloud console.</li> <li>• <b>Connection Status</b> Displays the connection status for assets, events, and the connector.</li> <li>• <b>Last Connection Time</b> Displays the last connection time for assets, events, and the connector.</li> <li>• <b>Last Connection Error</b> Displays the last connection error for assets, events, and the connector.</li> </ul> <p><b>Enrollment Information</b> contains the following fields:</p> <ul style="list-style-type: none"> <li>• <b>Enrollment Status</b> Displays the enrollment status with the cloud console.</li> <li>• <b>Date/Time of Enrollment</b> Displays when the Symantec Endpoint Protection Manager domain was enrolled with the cloud console.</li> <li>• <b>Customer ID</b> Your customer ID used for the cloud enrollment.</li> <li>• <b>Domain ID</b> The ID of the Symantec Endpoint Protection Manager domain that is enrolled with the cloud console.</li> </ul> <p><b>Note:</b> When the domain is enrolled in the cloud, the cloud console inheritance structure applies to the policies that it manages.</p> <p>For help with proxy error messages, see <a href="#">Proxy error messages appear in the Endpoint Protection Manager Cloud tab &gt; Troubleshooting</a> .</p>
<b>Feature Visibility</b>	<p>Turn these options so that the Symantec Endpoint Protection Manager retrieves and refreshes this data from the cloud. If the SEPM is unenrolled or does not connect to the cloud, the data still refreshes. Turn off the toggle if you do not want the data to refresh for performance reasons.</p> <p>Turn off these options if you don't want your SEPM information to go up to the Cloud, and yes, if they don't want the impact of the downloaded data in terms of network bandwidth and impact to the SEPM database, since we are inserting more data into their database.</p> <p>SEPM information to go up to the Cloud, and yes, if they don't want the impact of the downloaded data in terms of network bandwidth and impact to the SEPM database, since we are inserting more data into their database.</p>

---

## Related Documents

---

Download Symantec Endpoint Protection guides and manuals as PDF files

### Symantec Endpoint Protection Documentation:

- Current release:
  - [Symantec Endpoint Protection Quick Start](#)
  - [Symantec Endpoint Protection 14.3 RU2 for Installation and Administration Guide](#)
  - [Symantec Endpoint Protection 14.3 RU2 for Mac Client Guide](#)
  - [Symantec Endpoint Protection 14.3 RU2 for Linux Client Guide](#)
  - [Symantec Endpoint Protection Manager REST API Reference](#)
- Release Notes:
  - [Symantec Endpoint Protection 14.3.2 \(14.3 RU2\) Release Notes](#) (last updated: July 1, 2021)
  - [Symantec Endpoint Protection 14.3.1.1 \(14.3 RU1 MP1\) Release Notes](#)
  - [Symantec Endpoint Protection 14.3.1 \(14.3 RU1\) Release Notes](#)
  - [Symantec Endpoint Protection 14.3.0.1 \(14.3 MP1\) Release Notes](#)
  - [Symantec Endpoint Protection 14.3 Release Notes](#)
  - [Symantec Endpoint Protection 14.2.x Release Notes \(.zip\)](#)
  - [Symantec Endpoint Protection 14.x/14.1 Release Notes \(.zip\)](#)
  - [Symantec Endpoint Protection 12.1.6.10 Release Notes](#)
- Previous releases:
  - [Symantec Endpoint Protection Sizing and Scalability Best Practices Whitepaper](#)
  - [Symantec Endpoint Protection 14.3 RU1 for Installation and Administration Guide](#)
  - [Symantec Endpoint Protection 14.3 RU1 for Mac Client Guide](#)
  - [Symantec Endpoint Protection 14.3 RU1 for Linux Client Guide](#)
  - [Symantec Endpoint Protection 14.3 for Mac Client Guide](#)
  - [Symantec Endpoint Protection 14.2.1 Documents \(.zip\)](#)
  - [Symantec Endpoint Protection 14.2 Documents \(.zip\)](#)
  - [Symantec Endpoint Protection 14 Documents \(.zip\)](#)
  - [Symantec Endpoint Protection 14.2.x Tools \(.zip\)](#)
  - [Symantec Endpoint Protection Web Service SDK](#)
- Database Schema Reference:
  - [Symantec Endpoint Protection 14.3.2 Database Schema Reference](#)
  - [Symantec Endpoint Protection 14.3.1.1 Database Schema Reference](#)
  - [Symantec Endpoint Protection 14.3.1 Database Schema Reference](#)
  - [Symantec Endpoint Protection 14.3.0.1 Database Schema Reference](#)
  - [Symantec Endpoint Protection 14.2.2 to 14.3 Database Schema Reference](#)
  - [Symantec Endpoint Protection 14.2.1 to 14.2.1.1 Database Schema Reference](#)
  - [Symantec Endpoint Protection 14.2.1 Database Schema Reference](#)
  - [Symantec Endpoint Protection 14.2 Database Schema Reference](#)
- Third Party License Agreements:
  - [Symantec Endpoint Protection 14.3.1 to 14.3.2 Third Party License Agreements](#)

---

## Copyright statement

---

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom.

Copyright ©2021 Broadcom. All Rights Reserved.

The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit [www.broadcom.com](http://www.broadcom.com).

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.



